1. Γενικές Πληροφορίες

1.1 Εισαγωγή

Η σημαντική αύξηση των διασυνοριακών ροών δεδομένων προσωπικού χαρακτήρα, οι ραγδαίες τεχνολογικές εξελίξεις, η παγκοσμιοποίηση και το γεγονός, ότι τα ίδια τα φυσικά πρόσωπα δημοσιοποιούν ολοένα και ευκολότερα τα προσωπικά τους δεδομένα μέσα από τις ιστοσελίδες κοινωνικής δικτύωσης, δημιουργούν νέες προκλήσεις για την προστασία των προσωπικών δεδομένων. Οι εξελίξεις αυτές οδήγησαν μεταξύ άλλων σύμφωνα με τις αιτιολογικές σκέψεις του **Γενικού Κανονισμού Προστασίας Δεδομένων (GPDR)** στην ανάγκη θέσπισης αυτού.

Ο GDPR υιοθετήθηκε προκειμένου να μην υπάρχουν διαφορές μεταξύ των κρατών μελών στους νόμους προστασίας των δεδομένων προσωπικού χαρακτήρα και για να αναμορφώσει τον τρόπο που οι οργανώσεις προσεγγίζουν τα προσωπικά δεδομένα. **Ο Κανονισμός ενισχύει τα θεμελιώδη δικαιώματα των ευρωπαίων κατοίκων για τα προσωπικά τους δεδομένα και ελέγχει υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία, όταν είναι υπεύθυνοι για την παραβίαση του GPDR.**

Ο Κανονισμός (GDPR 2016/679) θα είναι άμεσα εφαρμοστέος σε όλα τα κράτη μέλη της ΕΕ με ημερομηνία εφαρμογής του νόμου **την 25η Μαΐου 2018.** Αντικαθιστά την Οδηγία 95/46/ΕΚ που αφορούσε στην προστασία των δεδομένων, η οποία είχε υιοθετηθεί στην Ελλάδα με το νόμο 2472/1997.

Απαιτείται δε ιδιαίτερη προσοχή καθώς η μη συμμόρφωση στις διατάξεις του, επισύρει πολύ σοβαρά διοικητικά πρόστιμα από την αρμόδια Εποπτική Αρχή, τα οποία μπορούν να φθάσουν ανάλογα με τις διατάξεις που παραβιάζονται έως 20.000.000 Ευρώ ή σε περίπτωση επιχειρήσεων έως το 4% του συνολικού παγκοσμίου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους ανάλογα με το ποιο είναι υψηλότερο.

Ο Κανονισμός ισχύει για όλα τα υποκείμενα δεδομένων (πρόσωπα) εντός της ΕΕ, αλλά αφορά και οργανώσεις που βρίσκονται εκτός της ΕΕ, εφόσον παρακολουθούν ή επεξεργάζονται προσωπικά δεδομένα κατά τη διάρκεια των συναλλαγών τους.

1.2 Ορισμοί

- **«Υποκείμενο Δεδομένων»:** Κάθε φυσικό πρόσωπο του οποίου τα προσωπικά δεδομένα επεξεργάζεται η ΕΤΑΙΡΕΙΑ.

- **«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 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,
- **Ειδικές κατηγορίες προσωπικών δεδομένων:** φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή η συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.
- **«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.
- **«κατάρτιση προφίλ»:** οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου,
- **«υπεύθυνος επεξεργασίας»:** 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·,
- **«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 της επεξεργασίας,
- **«αποδέκτης»:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι.
- **«συγκατάθεση» του υποκειμένου των δεδομένων:** κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν,

- **«παραβίαση δεδομένων προσωπικού χαρακτήρα»:** η 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.

1.3 Σκοπός

Η σύννομη επεξεργασία και προστασία των προσωπικών δεδομένων των υποκειμένων που επεξεργάζεται η ΕΤΑΙΡΕΙΑ. Η παρούσα πολιτική έχει ως στόχο την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων.

1.4 Πεδίο Εφαρμογής

Η παρούσα πολιτική ισχύει για κάθε επεξεργασία προσωπικών δεδομένων που εκτελεί η ΕΤΑΙΡΕΙΑ.

2. Περιγραφή Πολιτικής

2.1 Η ΕΤΑΙΡΕΙΑ δεσμεύεται να συμμορφώνεται με όλους τους σχετικούς νόμους της ΕΕ και της Ελλάδας που αφορούν τα προσωπικά δεδομένα και την προστασία των "δικαιωμάτων και των ελευθεριών" των υποκειμένων σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

2.2 Η ΕΤΑΙΡΕΙΑ έχει αναπτύξει και εφαρμόζει την Πολιτική Προστασίας Δεδομένων καθώς και κάθε άλλη απαραίτητη πολιτική και διαδικασία σχετικά την επεξεργασία και την προστασία των προσωπικών δεδομένων.

2.3 Η Πολιτική Προστασίας Προσωπικών Δεδομένων ισχύει για κάθε επεξεργασία προσωπικών δεδομένων της ΕΤΑΙΡΕΙΑΣ, συμπεριλαμβανομένων των προσωπικών δεδομένων των πελατών, των εργαζομένων, των προμηθευτών, των συνεργατών και οποιωνδήποτε άλλων προσωπικών δεδομένων φυσικών προσώπων επεξεργάζεται η ΕΤΑΙΡΕΙΑ.

2.4 Ο Υπεύθυνος επεξεργασίας οφείλει να ενημερώνει τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ) για τυχόν αλλαγές στους σκοπούς επεξεργασίας των δεδομένων και ο ΥΠΔ αντανακλά τις αλλαγές αυτές στο αρχείο.

2.5 Η πολιτική αυτή ισχύει για όλους τους υπαλλήλους και τους συνεργάτες της ΕΤΑΙΡΕΙΑΣ. Κάθε παραβίαση των ΠΔ που έχει επίπτωση στα υποκείμενα θα αναφερθεί το συντομότερο δυνατόν στην ΑΠΔΠΧ.

2.6 Η ΕΤΑΙΡΕΙΑ θα πρέπει να καθορίσει τους στόχους για την προστασία των δεδομένων.

2.7 Οι Συνεργάτες και τυχόν τρίτα μέρη που συνεργάζονται με ή για την ΕΤΑΙΡΕΙΑ και έχουν πρόσβαση σε προσωπικά δεδομένα, θα πρέπει να διαβάσουν, να κατανοήσουν και να συμμορφωθούν πλήρως με αυτήν την πολιτική. Κανένα τρίτο μέρος δεν μπορεί να έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται η ΕΤΑΙΡΕΙΑ χωρίς την υπογραφή της σύμβασης συνεργασίας και της εμπιστευτικότητας.

2.8 Η επικοινωνία με τα υποκείμενα για προωθητικές ενέργειες γίνεται μέσω της πολιτικής επικοινωνίας με υποκείμενα μέσω ηλεκτρονικών μέσων.

2.9 Η ΕΤΑΙΡΕΙΑ έχει αναπτύξει τον κανονισμό χρήσης επικοινωνιακών μέσων και μέσων ηλεκτρονικής επεξεργασίας που χρησιμοποιούν οι εργαζόμενοι στους χώρους ή για τους σκοπούς της εργασίας ή έχουν διατεθεί σε αυτούς από την ΕΤΑΙΡΕΙΑ. Ο κανονισμός αυτός έχει κοινοποιηθεί στους εργαζομένους.

3. Ρόλοι και Αρμοδιότητες

3.1 Η ΕΤΑΙΡΕΙΑ είναι, σύμφωνα με τον Κανονισμό, Υπεύθυνος Επεξεργασίας.
3.2 Η ΕΤΑΙΡΕΙΑ φέρει την ευθύνη και είναι σε θέση να αποδείξει την συμμόρφωση της με τον Κανονισμό.
3.3 Η συμμόρφωση με τη νομοθεσία περί προστασίας δεδομένων είναι ευθύνη όλων των υπαλλήλων που επεξεργάζονται τα προσωπικά δεδομένα.
3.4 Η Πολιτική Εκπαίδευσης της ΕΤΑΙΡΕΙΑΣ (GDPR_Πολιτική Εκπαίδευσης) καθορίζει τις απαραίτητές κατευθύνσεις για την κατάρτιση και την ευαισθητοποίηση των υπαλλήλων για την επεξεργασία και την προστασία των προσωπικών δεδομένων.

3.5 Έχουν καθορισθεί οι απαραίτητοι ρόλοι και αρμοδιότητες. Πιο συγκεκριμένα:

3.5.1 Η Διοίκηση:

- Εγκρίνει τους μηχανισμούς συμμόρφωσης και διαχείρισης της επικινδυνότητας.
- Επικυρώνει την πολιτική προστασίας των προσωπικών δεδομένων και την πολιτική ασφαλείας.
- Ανακοινώσει στους υπαλλήλους, στους πελάτες και στους συνεργάτες την σπουδαιότητα της προστασίας των προσωπικών δεδομένων και την ενεργή υποστήριξη της στην συμμόρφωση με τον νέο κανονισμό (αποστολή e-mail, ανακοίνωση στον ιστότοπο).

3.5.2 Ο Υπεύθυνος προστασίας Δεδομένων:

- Αναφέρεται στην Διοίκηση για θέματα επεξεργασίας και προστασίας προσωπικών δεδομένων.

- Ενημερώνει και να συμβουλεύει την ΕΤΑΙΡΕΙΑ για την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων,
- Ενεργεί ως σημείο επικοινωνίας και συνεργάζεται με την ΑΠΔΠΧ για ζητήματα που σχετίζονται με την επεξεργασία.
- Τα στοιχεία του γνωστοποιούνται στην ΑΠΔΠΧ.

3.5.3 Ο Εσωτερικός Έλεγχος:

- Επιθεωρεί τους μηχανισμούς συμμόρφωσης και προστασίας των προσωπικών δεδομένων

3.5.4 Οι Διευθυντές και οι Προϊστάμενοι:

- Παρακολουθούν την συμμόρφωση των υφισταμένων τους με την πολιτική ασφαλείας.

3.5.5 Ο Διευθυντής Πληροφορικής:

- Υλοποιεί και να διαχειρίζεται τους τεχνικούς μηχανισμούς συμμόρφωσης και προστασίας στις καθημερινές λειτουργίες των συστημάτων.

3.5.6 Ο Διευθυντής Ανθρώπινου Δυναμικού:

- Υλοποιεί τις διαδικασίες συμμόρφωσης και προστασίας του ανθρώπινου δυναμικού.
- Υλοποιεί το κατάλληλο πρόγραμμα εκπαίδευσης και ευαισθητοποίησης του προσωπικού.

3.5.7 Οι υπάλληλοι:

- Είναι υπεύθυνοι για την εξασφάλιση της ακρίβειας και της ενημέρωσης των οποιωνδήποτε προσωπικών δεδομένων τους και τα οποία παρέχονται στην ΕΤΑΙΡΕΙΑ.

4. Βασικές Αρχές Επεξεργασίας Προσωπικών Δεδομένων

Η επεξεργασία των προσωπικών δεδομένων διεξάγεται σύμφωνα με τις αρχές προστασίας δεδομένων που ορίζονται στο άρθρο 5 του Κανονισμού. Όλες οι πολιτικές καθώς και οι διαδικασίες έχουν σχεδιασθεί για να εξασφαλίσουν την συμμόρφωση με τις αρχές αυτές.

4.1 Τα προσωπικά δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»).

4.1.1 Η ΕΤΑΙΡΕΙΑ θα πρέπει να προσδιορίσει την νομιμότητα της επεξεργασίας πριν την επεξεργασία των προσωπικών δεδομένων και θα καταχωρίσει κάθε απαραίτητη πληροφορία στο αρχείο δραστηριοτήτων της επεξεργασίας (Διαδικασία Διαχείριση της επεξεργασίας των προσωπικών δεδομένων).

4.1.2 Ο Κανονισμός περιλαμβάνει κανόνες για την πληροφόρηση των υποκειμένων για την επεξεργασία των προσωπικών τους δεδομένων (άρθρα 12, 13 και 14). Οι πληροφορίες πρέπει να κοινοποιούνται στο υποκείμενο των δεδομένων σε κατανοητή μορφή με σαφή και απλή γλώσσα. Η διαδικασία επεξεργασίας προσωπικών δεδομένων καθορίζεται στο έγγραφο «Διαχείριση της επεξεργασίας των προσωπικών δεδομένων» και η Ενημέρωση των Υποκειμένων στο έντυπο «Δήλωση Προστασίας των Προσωπικών Δεδομένων».

4.2 Τα προσωπικά δεδομένα θα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς·

4.2.1 Τα δεδομένα που λαμβάνονται για καθορισμένους σκοπούς δεν πρέπει να χρησιμοποιούνται για σκοπούς διαφορετικούς από εκείνους που αναφέρονται στο αρχείο δραστηριοτήτων της επεξεργασίας των προσωπικών δεδομένων (Διαδικασία Διαχείρισης της επεξεργασίας των προσωπικών δεδομένων).

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

4.3.1 Η ΕΤΑΙΡΕΙΑ θα πρέπει να συλλέγει τις απόλυτα απαραίτητες πληροφορίες για τον σκοπό της επεξεργασίας (βλέπε Έντυπο GDPR_Αρχείο δραστηριοτήτων της επεξεργασίας).

4.3.2 Όλα τα έντυπα συλλογής δεδομένων (ηλεκτρονικά ή σε έντυπα), πρέπει να περιλαμβάνουν την ενημέρωση για την επεξεργασία προσωπικών δεδομένων και να εγκρίνονται από τον υπεύθυνο προστασίας δεδομένων.

4.3.3 Η ΕΤΑΙΡΕΙΑ θα μεριμνήσει ώστε σε ετήσια βάση όλες οι διαδικασίες καθώς και οι μέθοδοι συλλογής δεδομένων να επανεξεταστούν από τον εσωτερικό ελεγκτή προκειμένου να διασφαλιστεί ότι τα συλλεγόμενα δεδομένα εξακολουθούν να είναι επαρκή, συναφή και όχι υπερβολικά (Διαδικασία Εκπόνησης Εκτίμησης Αντικτύπου).

4.4 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»),

4.4.1 Τα δεδομένα που αποθηκεύονται από τον υπεύθυνο επεξεργασίας δεδομένων θα πρέπει να επανεξετάζονται ετησίως και να τροποποιούνται όπως απαιτείται. Δεν πρέπει να διατηρούνται μη ακριβή δεδομένα.

4.4.2 Η ΕΤΑΙΡΕΙΑ είναι υπεύθυνη ότι εκπαιδεύει το προσωπικό για τη σημασία της ακρίβειας των δεδομένων κατά την συλλογή τους και την διαχείριση τους.

4.4.3 Είναι ευθύνη του υποκειμένου των δεδομένων να διασφαλίσει ότι τα δεδομένα που κατέχει η ΕΤΑΙΡΕΙΑ είναι ακριβή και ενημερωμένα. Η συμπλήρωση ενός εντύπου εγγραφής ή αίτησης από ένα υποκείμενο των δεδομένων θα περιλαμβάνει δήλωση ότι τα δεδομένα που περιέχονται σε αυτό είναι ακριβή κατά την ημερομηνία υποβολής.
4.4.4 Τα υποκείμενα (εργαζόμενοι, πελάτες , συνεργάτες) θα πρέπει να ενημερώνουν την ΕΤΑΙΡΕΙΑ για οποιεσδήποτε αλλαγές στα προσωπικά τους δεδομένα ώστε να είναι δυνατή η ενημέρωση των αντίστοιχων αρχείων. Η ΕΤΑΙΡΕΙΑ θα πρέπει να τους παρέχει τις απαραίτητες οδηγίες για την διαδικασία τροποποίησης των δεδομένων.
4.4.5 Η ΕΤΑΙΡΕΙΑ είναι υπεύθυνος για τη ανάπτυξη των κατάλληλων διαδικασιών και πολιτικών για την ακρίβεια των δεδομένων, λαμβάνοντας υπόψη τον όγκο των δεδομένων που συλλέγονται, την ταχύτητα με την οποία μπορεί να τροποποιηθούν και οποιαδήποτε άλλους συναφείς παράγοντες.
4.4.6 Μία φορά το έτος, η ΕΤΑΙΡΕΙΑ θα εξετάσει τις ημερομηνίες διατήρησης των προσωπικών δεδομένων που επεξεργάζεται και θα προσδιορίσει τυχόν δεδομένα που δεν απαιτούνται πλέον το πλαίσιο του σκοπού επεξεργασίας. Αυτά τα δεδομένα θα διαγραφούν / καταστραφούν με ασφαλή τρόπο.
4.4.7 Ο υπεύθυνος προστασίας δεδομένων είναι υπεύθυνος για την απάντηση σε αιτήματα για τροποποίηση των προσωπικών δεδομένων από τα υποκείμενα των δεδομένων εντός ενός μηνός. Αυτό μπορεί να επεκταθεί σε δύο επιπλέον μήνες για περίπλοκα αιτήματα. Εάν η ΕΤΑΙΡΕΙΑ αποφασίσει να μην τροποποιήσει τα δεδομένα, ο υπεύθυνος προστασίας δεδομένων θα πρέπει να αιτιολογήσει στο υποκείμενο την απόφαση της ΕΤΑΙΡΕΙΑΣ και να τον ενημερώσει για το δικαίωμά του να υποβάλει καταγγελία στην ΑΠΔΠΧ.
4.4.8 Σε περίπτωση που συνεργάτες της ΕΤΑΙΡΕΙΑΣ μεταβιβάσει ανακριβή ή παρωχημένα προσωπικά δεδομένα, ο η ΕΤΑΙΡΕΙΑ είναι υπεύθυνος για την ενημέρωση των συνεργατών σχετικά με τα υποκείμενα και τα δεδομένα που πρέπει να τροποποιηθούν.

4.5 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·

4.5.1 Όταν τα προσωπικά δεδομένα διατηρούνται πέρα από την ημερομηνία επεξεργασίας, θα ανωνυμοποιηθούν ή θα καταστραφούν προκειμένου να προστατευθεί η ταυτότητα του προσώπου στο οποίο αναφέρονται τα δεδομένα σε περίπτωση παραβίασης των δεδομένων.

4.5.2 Τα προσωπικά δεδομένα θα διατηρηθούν σύμφωνα με τη Διαδικασία Διατήρησης των Αρχείων και, μόλις περατωθεί η ημερομηνία διατήρησής τους, θα πρέπει να καταστραφούν με ασφάλεια σύμφωνα με την Διαδικασία Ασφαλούς Καταστροφής.

4.5.3 Ο υπεύθυνος προστασίας δεδομένων θα πρέπει να εγκρίνει συγκεκριμένα κάθε διατήρηση δεδομένων πέρα της περιόδους διατήρησης τους και πρέπει να εξασφαλίζει ότι η αιτιολόγηση είναι σαφώς προσδιορισμένη και σύμφωνα με τις απαιτήσεις της νομοθεσίας. Η έγκριση αυτή πρέπει να είναι καταγεγραμμένη.

4.6 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»).

4.6.1 Ο υπεύθυνος προστασίας δεδομένων θα προβεί σε εκτίμηση επικινδυνότητας λαμβάνοντας υπόψη όλες τις δραστηριότητες της επεξεργασίας της ΕΤΑΙΡΕΙΑΣ. Για τον προσδιορισμό των κατάλληλων μηχανισμών θα πρέπει επίσης να εξεταστεί η έκταση της πιθανής ζημίας ή απώλειας που μπορεί να προκληθεί σε άτομα (π.χ. προσωπικό ή πελάτες) σε περίπτωση παραβίασης της ασφάλειας, καθώς και τυχόν ζημιές για τη φήμη, συμπεριλαμβανομένης της πιθανής απώλειας εμπιστοσύνης των πελατών.

4.6.2 Οι μηχανισμοί ελέγχου προστασίας των προσωπικών δεδομένων αναφέρονται στην δήλωση εφαρμογής.

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

4.7.1 Η ΕΤΑΙΡΕΙΑ θα πρέπει να αποδείξει την συμμόρφωση με τον Κανονισμό, εφαρμόζοντας τις κατάλληλες πολιτικές, τεχνικά και οργανωτικά μέτρα, καθώς και υιοθετώντας τεχνικές όπως η προστασία δεδομένων από σχεδιασμό, διαδικασίες διαχείρισης περιστατικών ασφαλείας κ.λπ. (Κατάλογος Ελεγχόμενων Εγγράφων και Δήλωση Εφαρμοσιμότητας)

5. Δικαιώματα των υποκειμένων

5.1Τα υποκείμενα των δεδομένων έχουν τα ακόλουθα δικαιώματα όσον αφορά την επεξεργασία δεδομένων:

5.1.1 Δικαίωμα ενημέρωσης (άρθρα 12, 13 και 14). Πληροφορίες που πρέπει να παρέχονται στο υποκείμενο δεδομένων(πχ ταυτότητα του υπεύθυνου επεξεργασίας, σκοπούς και νομική βάση επεξεργασίας κ.α.)

5.1.2 Δικαίωμα πρόσβασης (άρθρα 14). Λήψη επιβεβαίωσης για την επεξεργασία ή μη των δεδομένων προσωπικού χαρακτήρα που αφορούν το υποκείμενο. Εάν υφίστανται επεξεργασία τότε δύναται να ασκήσει το δικαίωμα πρόσβασης στα δεδομένα αυτά.

5.1.3 Δικαίωμα στη διόρθωση δεδομένων (άρθρο. 15). Δικαίωμα του υποκειμένου να απαιτήσει τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν είτε τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα.

5.1.3 Δικαίωμα στη λήθη (άρθρο 16). Δικαίωμα του υποκειμένου να αιτηθεί τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν για τους αναφερόμενους στον κανονισμό λόγους.

5.1.4 Δικαίωμα στον περιορισμό της επεξεργασίας (άρθρο 18). Το υποκείμενο δύναται να αιτηθεί τον περιορισμό της επεξεργασίας όταν ισχύει ένας από τους περιοριστικά αναφερόμενους στον κανονισμό λόγους.

5.1.5 Δικαίωμα στη φορητότητα των δεδομένων (άρθρο 20). Δικαίωμα του υποκειμένου να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας και να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας.

5.1.6 Δικαίωμα αντίρρησης/εναντίωσης (άρθρο 21). Δικαίωμα του υποκειμένου στην πρόσβαση σε διοικητικές και δικαστικές διαδικασίες προκειμένου είτε να προσβάλλουν μη νόμιμες επεξεργασίες είτε να διεκδικήσουν την επανόρθωση της βλάβης που έχουν υποστεί.

5.1.7 Δικαίωμα αντίρρησης στις περιπτώσεις profiling (άρθρο 22). Δικαίωμα του υποκειμένου να προσβάλλει μη νόμιμες επεξεργασίες σε περιπτώσεις profiling.

5.2 Η ΕΤΑΙΡΕΙΑ θα πρέπει να εξασφαλίζει ότι τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα ανωτέρω δικαιώματα.

5.2.1 Τα υποκείμενα των δεδομένων (Διαδικασία διαχείρισης αιτημάτων των υποκειμένων) μπορούν να υποβάλλουν:

- Αιτήματα πρόσβασης δεδομένων.
- Αιτήματα Τροποποίησης Προσωπικών Δεδομένων
- Αιτήματα Διαγραφής δεδομένων
- Αιτήματα Περιορισμού της Επεξεργασίας
- Αιτήματα φορητότητας των δεδομένων
- Αιτήματα Αντίρρησης/Εναντίωσης

5.2.2 Η εταιρεία έχει αναπτύξει την διαδικασία διαχείρισης αιτημάτων των υποκειμένων έτσι ώστε να διαχειριστεί τα αιτήματα τους.

6. Συγκατάθεση

6.1 Όταν η επεξεργασία βασίζεται σε συγκατάθεση, η ΕΤΑΙΡΕΙΑ είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα.

6.2 Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση.

6.2 Η ΕΤΑΙΡΕΙΑ κατανοεί τις προϋποθέσεις και τη νομιμότητα της «συγκατάθεσης» που σημαίνει ότι το υποκείμενο των δεδομένων έχει ενημερωθεί πλήρως για την επεξεργασία των προσωπικών δεδομένων (Έντυπο Ενημέρωσης για την Επεξεργασία Προσωπικών Δεδομένων) και ότι έχει δώσει τη συναίνεση του, χωρίς να του ασκηθούν πιέσεις. Η συναίνεση που αποκτάται υπό την πίεση ή βάσει παραπλανητικών πληροφοριών δεν αποτελεί έγκυρη βάση για την επεξεργασία.

6.3. Η συγκατάθεση προσωπικών δεδομένων ειδικού χαρακτήρα πρέπει να είναι ρητή (Διαδικασία Διαχείρισης της Επεξεργασίας Προσωπικών Δεδομένων, Έντυπο Ρητής Συγκατάθεσης, Έντυπο Ενημέρωσης για την επεξεργασία προσωπικών Δεδομένων).

6.3Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της (Διαδικασία Διαχείρισης Αιτήσεων Ατης Συγκατάθεσης).

6.4 Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

6.5 Η συγκατάθεση για παιδιά ηλικίας κάτω των 16 ετών, είναι σύννομη μόνο εάν η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού.

6.6. Η εταιρεία για την ηλεκτρονική συγκατάθεση θα υιοθετήσει την πολιτική ηλεκτρονικής συγκατάθεσης.

7. Ασφάλεια Δεδομένων Προσωπικού Χαρακτήρα

Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, η ΕΤΑΙΡΕΙΑ εφαρμόζουν

κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων:

7.1 Έχει καταγράψει τις δραστηριότητες της επεξεργασίας στο Αρχείο Δραστηριοτήτων της Επεξεργασίας (Διαδικασία Διαχείρισης της επεξεργασίας, Έντυπο Αρχείο Δραστηριοτήτων της Επεξεργασίας).

7.2 Έχει εκπονήσει όπου απαιτείται Εκτίμηση του Αντίκτυπου (Διαδικασία Εκπόνησης Εκτίμησης του Αντίκτυπου).

7.3 Έχει Εφαρμόσει τα κατάλληλα Τεχνικά και Οργανωτικά μέτρα (Έντυπο Δήλωση Εφαρμοσιμότητας) για την προστασία των προσωπικών δεδομένων και την διαχείριση της επικινδυνότητας (Ανάλυση Αποκλίσεων και Πλάνο Συμμόρφωσης) συμπεριλαμβανομένων τεχνολογιών κρυπτογράφησης, προστασίας από ιούς, συστήματα τείχους προστασίας, προστασίας εξ ορισμού και από τον σχεδιασμό.

8. Εμπιστευτικότητα Δεδομένων

8.1 Η ΕΤΑΙΡΕΙΑ πρέπει να διασφαλίζει ότι τα προσωπικά δεδομένα δεν αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα, συμπεριλαμβανομένων μελών της οικογένειας, φίλων κ.λπ. Όλοι οι υπάλληλοι θα πρέπει να είναι προσεκτικοί όταν καλούνται να αποκαλύψουν προσωπικά δεδομένα που επεξεργάζεται η ΕΤΑΙΡΕΙΑ σε τρίτα άτομα και θα πρέπει να ταυτοποιήσουν το υποκείμενο. Οι υπάλληλοι θα πρέπει να παρακολουθήσουν ειδική εκπαίδευση που τους επιτρέπει να αντιμετωπίσουν αποτελεσματικά τον εν λόγω κίνδυνο. Είναι σημαντικό να έχουμε κατά νου κατά πόσον η αποκάλυψη των πληροφοριών είναι σχετική και αναγκαία για τη διεξαγωγή των δραστηριοτήτων της ΕΤΑΙΡΕΙΑΣ.

8.2. Η ΕΤΑΙΡΕΙΑ θα πρέπει να υπογράψει με όλους τους συνεργάτες και το προσωπικό της συμβάσεις εμπιστευτικότητας.

9. Διατήρηση και διάθεση προσωπικών δεδομένων

9.1 Η ΕΤΑΙΡΕΙΑ δεν διατηρεί τα προσωπικά δεδομένα σε μορφή που επιτρέπει τον προσδιορισμό των υποκειμένων των δεδομένων για μεγαλύτερο χρονικό διάστημα από αυτό που είναι αναγκαίο, σε σχέση με τον (τους) σκοπό (ους) για τον οποίο συλλέχθηκαν αρχικά τα δεδομένα.

9.2 Η ΕΤΑΙΡΕΙΑ μπορεί να αποθηκεύει προσωπικά δεδομένα για μεγαλύτερο χρονικό διάστημα από το χρονικό διάστημα που είναι αναγκαίο για τον (τους) σκοπό (ούς) εάν τα προσωπικά δεδομένα θα υποβληθούν σε επεξεργασία αποκλειστικά για λόγους αρχειοθέτησης, για λόγους δημόσιου συμφέροντος, επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, με την εφαρμογή των κατάλληλων τεχνικών

και οργανωτικών μέτρων για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

9.3 Η περίοδος διατήρησης για κάθε κατηγορία δεδομένων προσωπικού χαρακτήρα θα καθορίζεται στη Έντυπο Διατήρησης των Αρχείων μαζί με τα κριτήρια που χρησιμοποιούνται για τον προσδιορισμό αυτής της περιόδου, συμπεριλαμβανομένων τυχόν υποχρεωτικών νομικών υποχρεώσεων της ΕΤΑΙΡΕΙΑΣ.

9.4 Η διάθεση δεδομένων θα γίνεται σύμφωνα με τη Διαδικασία Ασφαλούς Διάθεσης.

10. Διαβίβαση Προσωπικών Δεδομένων προς τρίτες χώρες ή διεθνείς οργανισμούς

10.1 Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό μπορεί να πραγματοποιηθεί σύμφωνα με την Διαδικασία Διαβίβασης Προσωπικών Δεδομένων σε Τρίτη Χώρα.

11. Καταγραφή των Δραστηριοτήτων της Επεξεργασίας και Εκπόνηση της Εκτίμησης του Αντίκτυπου στην ιδιωτικότητα

11.1 Η ΕΤΑΙΡΕΙΑ καταγράφει κάθε δραστηριότητα της επεξεργασίας των προσωπικών δεδομένων ως τμήμα της διαδικασίας εκπόνησης εκτίμησης του αντίκτυπου στην ιδιωτικότητα σε αρχείο (Αρχείο Δραστηριοτήτων της Επεξεργασίας).

11.2. Το εν λόγω αρχείο περιλαμβάνει όλες τις ακόλουθες πληροφορίες:

- τους σκοπούς της επεξεργασίας,
- περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,
- τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,
- όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού και, σε περίπτωση διαβιβάσεων που αναφέρονται στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο του Κανονισμού της τεκμηρίωσης των κατάλληλων εγγυήσεων,
- όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διάφορων κατηγοριών δεδομένων,

- όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 του Κανονισμού, παράγραφος 1.

11.3 Η ΕΤΑΙΡΕΙΑ θα πρέπει να θέσει το αρχείο στη διάθεση της ΑΠΔΠΧ αρχής κατόπιν αιτήματος.

11.4 Η ΕΤΑΙΡΕΙΑ προσδιορίζει και αξιολογεί τους κινδύνους για τα υποκείμενα που συνδέονται με την επεξεργασία των προσωπικών δεδομένων σύμφωνα με την διαδικασία εκπόνησης εκτίμησης του αντίκτυπου στην ιδιωτικότητα.

12. Διαχείριση Περιστατικών Παραβίασης Προσωπικών Δεδομένων

12.1 Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, η ΕΤΑΙΡΕΙΑ γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην ΑΠΔΠΧ, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην ΑΠΔΠΧ δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

12.1.1 Η διαχείριση των περιστατικών ασφαλείας καθώς και η γνωστοποίηση της παραβίασης των προσωπικών δεδομένων περιγράφονται στην Διαδικασία Διαχείρισης Περιστατικών Ασφαλείας.

13. Εκτελούντες την Επεξεργασία

13.1 Η ΕΤΑΙΡΕΙΑ χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του Κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.

13.1.1 Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με την ΕΤΑΙΡΕΙΑ και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας.

13.2 Ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια της ΕΤΑΙΡΕΙΑΣ.