



---

DPO-PeDaPro-1.0 21/04/2021  
Πολιτική για την Προστασία των  
Δεδομένων Προσωπικού  
Χαρακτήρα

---

**Απρίλιος 2021**



---

## ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

<b>1. ΕΙΣΑΓΩΓΗ</b> .....	4
<b>2. ΔΗΛΩΣΗ ΠΟΛΙΤΙΚΗΣ</b> .....	6
<b>3. ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ (ΣΔΠΠ - ΡΙΜΣ)</b> .....	6
<b>4. ΕΥΘΥΝΕΣ ΚΑΙ ΡΟΛΟΙ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR)</b> .....	7
<b>5. ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ</b> .....	8
<b>6. ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ</b> .....	12
<b>7. ΣΥΓΚΑΤΑΘΕΣΗ</b> .....	13
<b>8. ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ</b> .....	14
<b>9. ΓΝΩΣΤΟΠΟΙΗΣΗ ΔΕΔΟΜ'ΕΝΩΝ</b> .....	15
<b>10. ΔΙΑΤΗΡΗΣΗ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ</b> .....	15
<b>11. ΜΕΤΑΦΟΡΑ ΔΕΔΟΜ'ΕΝΩΝ</b> .....	16
<b>12. ΜΗΤΡΩΟ ΠΟΡΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ / ΑΠΟΓΡΑΦΗ ΔΕΔΟΜΕΝΩΝ</b> .....	17
<b>13. ΙΔΙΟΚΤΗΣΙΑ ΕΓΓΡΑΦΟΥ ΚΑΙ ΈΓΚΡΙΣΗ</b> .....	18

## 1. ΕΙΣΑΓΩΓΗ

### 1.1 Ιστορικό του Γενικού Κανονισμού για την προστασία των δεδομένων προσωπικού χαρακτήρα («GDPR»)

Ο Γενικός Κανονισμός για την προστασία των δεδομένων προσωπικού χαρακτήρα ΕΕ 2016/679 αντικαθιστά την Οδηγία της Ευρωπαϊκής Ένωσης (ΕΕ) για την προστασία των δεδομένων του 1995, όπως επίσης αντικαθιστά τις νομοθεσίες των επιμέρους κρατών μελών που αναπτύχθηκαν σύμφωνα με την οδηγία 95/46/ΕΚ για την προστασία των προσωπικών δεδομένων. Σκοπός του είναι να προστατεύσει τα "δικαιώματα και τις ελευθερίες" των φυσικών προσώπων (και να διασφαλίσει ότι τα προσωπικά δεδομένα δεν θα υποστούν επεξεργασία χωρίς τα ίδια τα υποκείμενα των δεδομένων να το γνωρίζουν και, όπου είναι δυνατόν, ότι τα δεδομένα προσωπικού χαρακτήρα θα τύχουν επεξεργασίας με τη συγκατάθεσή τους.

### 1.2 Ορισμοί που χρησιμοποιεί ο Όμιλος (προερχόμενοι από το GDPR)

Ουσιαστικό Πεδίο Εφαρμογής (Άρθρο 2) - το GDPR ισχύει για την επεξεργασία δεδομένων προσωπικού χαρακτήρα εν όλω ή εν μέρει με αυτοματοποιημένα μέσα (π.χ. με υπολογιστή) και την επεξεργασία, εκτός από αυτοματοποιημένα μέσα προσωπικών δεδομένων (π.χ. αρχεία εγγράφων), που αποτελούν μέρος ενός συστήματος αρχειοθέτησης ή προορίζονται να αποτελέσουν μέρος ενός συστήματος αρχειοθέτησης.

Εδαφικό Πεδίο Εφαρμογής (Άρθρο 3) - το GDPR θα εφαρμόζεται σε όλους τους υπεύθυνους επεξεργασίας που είναι εγκατεστημένοι στην ΕΕ οι οποίοι επεξεργάζονται τα προσωπικά δεδομένα των υποκειμένων των δεδομένων, στο πλαίσιο της εν λόγω εγκατάστασης. Θα ισχύει επίσης για τους υπεύθυνους επεξεργασίας εκτός της ΕΕ που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, προκειμένου να προσφέρουν αγαθά και υπηρεσίες ή να παρακολουθούν τη συμπεριφορά των υποκειμένων των δεδομένων που διαμένουν στην ΕΕ.

### 1.3 Ορισμοί του Άρθρου 4

Κύρια Εγκατάσταση - η κύρια εγκατάσταση του υπεύθυνου επεξεργασίας στην ΕΕ θα είναι ο τόπος στον οποίο ο υπεύθυνος της επεξεργασίας λαμβάνει τις βασικές αποφάσεις ως προς τον σκοπό και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Η κύρια εγκατάσταση ενός υπεύθυνου επεξεργασίας στην ΕΕ θα είναι το διοικητικό του κέντρο. Εάν ο υπεύθυνος επεξεργασίας είναι εγκατεστημένος εκτός της ΕΕ, θα πρέπει να διορίσει έναν αντιπρόσωπο στη διοικητική περιφέρεια στην οποία ο υπεύθυνος της επεξεργασίας δραστηριοποιείται, ώστε αυτός να ενεργεί για λογαριασμό του υπεύθυνου επεξεργασίας και να ασχολείται με τις εποπτικές αρχές.

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 - τα προσωπικά δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τις πολιτικές απόψεις, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστικές οργανώσεις και την επεξεργασία γενετικών δεδομένων, βιομετρικά δεδομένα με σκοπό τον μοναδικό εντοπισμό φυσικού προσώπου, δεδομένα σχετικά με την υγεία ή δεδομένα που αφορούν φυσικά πρόσωπα, σεξουαλική ζωή ή γενετήσιου προσανατολισμού.

Υπεύθυνος Επεξεργασίας - το φυσικό ή νομικό πρόσωπο, η Δημόσια Αρχή, η υπηρεσία ή άλλος φορέας που, μόνος 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.

Υποκείμενο των δεδομένων - κάθε άτομο εν ζωή που αποτελεί το αντικείμενο των προσωπικών δεδομένων που κατέχει ο Όμιλος Attica Group (εφεξής «Όμιλος»).

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.

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. Ο ορισμός αυτός συνδέεται με το δικαίωμα του υποκειμένου των δεδομένων να αντιτίθεται στη διαμόρφωση προφίλ και το δικαίωμα ενημέρωσης του υποκειμένου σχετικά με την ύπαρξη προφίλ, των μέτρων που βασίζονται στον προσδιορισμό του προφίλ και των προβλεπόμενων επιπτώσεων της συγκεκριμένης ανάλυσης στο άτομο.

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. Ο υπεύθυνος επεξεργασίας υποχρεούται να αναφέρει τις παραβιάσεις προσωπικών δεδομένων στην εποπτική αρχή, όταν η παραβίαση ενδέχεται να επηρεάσει αρνητικά τα προσωπικά δεδομένα ή την ιδιωτικότητα του υποκειμένου των δεδομένων.

Συγκατάθεση του Υποκειμένου των Δεδομένων - κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και με πλήρη επίγνωση, 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.

Παιδί – Ο Κανονισμός GDPR ορίζει ως παιδί κάθε πρόσωπο κάτω από την ηλικία των 16 ετών, αν και αυτό μπορεί να μειωθεί στα 13 έτη, ανά νομοθεσία κράτους μέλους. Η επεξεργασία των προσωπικών δεδομένων ενός παιδιού είναι νόμιμη μόνο αν έχει ληφθεί η γονική συγκατάθεση ή η συγκατάθεση του κηδεμόνα. Ο υπεύθυνος της επεξεργασίας καταβάλλει εύλογες προσπάθειες για να επαληθεύσει σε τέτοιες περιπτώσεις ότι ο έχων την γονική μέριμνα του παιδιού συγκατατίθεται ή επιτρέπει την επεξεργασία.

Τρίτος - οποιοδήποτε φυσικό ή νομικό πρόσωπο, Δημόσια Αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

Σύστημα αρχαιοθέτησης - κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο, είτε αποκεντρωμένο, είτε καταναμημένο σε λειτουργική ή γεωγραφική βάση.

## 2. ΔΗΛΩΣΗ ΠΟΛΙΤΙΚΗΣ

- 2.1 Ο Όμιλος, που εδρεύει στην Καλλιθέα, Λυσικράτους 1-7 & Ευριπίδου, δεσμεύεται για τη συμμόρφωση με όλους τους σχετικούς νόμους, τους Κανονισμούς και τις Οδηγίες της ΕΕ και της Ελλάδος, ως κράτος μέλος της Ευρωπαϊκής Ένωσης, όσον αφορά τα δεδομένα προσωπικού χαρακτήρα και την προστασία των «δικαιωμάτων και ελευθεριών» των ατόμων, των οποίων τα δεδομένα ο Όμιλος συλλέγει και επεξεργάζεται σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).
- 2.2 Η συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) περιγράφεται με αυτήν την πολιτική και άλλες σχετικές πολιτικές, όπως την Πολιτική Ασφάλειας Πληροφοριών, μαζί με τις σχετικές διαδικασίες του Ομίλου.
- 2.3 Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) και αυτή η πολιτική ισχύουν για όλες τις λειτουργίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα του Ομίλου, συμπεριλαμβανομένων εκείνων που εκτελούνται σε προσωπικά δεδομένα πελατών, εργαζομένων, προμηθευτών και συνεργατών και οποιωνδήποτε άλλων προσωπικών δεδομένων που επεξεργάζεται ο Όμιλος από οποιαδήποτε πηγή.
- 2.4 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/ΔΡΟ) είναι υπεύθυνος για την αναθεώρηση του αρχείου των δραστηριοτήτων επεξεργασίας ανά τακτά χρονικά διαστήματα, υπό το πρίσμα των οποιωνδήποτε αλλαγών στις δραστηριότητες του Ομίλου (όπως αυτές καθορίζονται από τις αλλαγές στο αρχείο των δραστηριοτήτων επεξεργασίας και μέσω της ανασκόπησης της διαχείρισης των δεδομένων αυτών) και σε τυχόν πρόσθετες απαιτήσεις που προσδιορίζονται μέσω της “Διαδικασίας Εκτίμησης Επιπτώσεων της Προστασίας Δεδομένων (ΕΕΠΔ-DPIA)”. Το αρχείο αυτό πρέπει να είναι διαθέσιμο κατόπιν αιτήματος της Εποπτικής Αρχής.
- 2.5 Η παρούσα πολιτική ισχύει για όλους τους εργαζομένους και συνεργαζόμενους τρίτους με τον Όμιλο, όπως προμηθευτές και παρόχους υπηρεσιών. Οποιαδήποτε παραβίαση του Κανονισμού GDPR θα αντιμετωπιστεί σύμφωνα με τις εσωτερικές διαδικασίες του Ομίλου και δύναται επίσης να αποτελέσει ποινικό αδίκημα, οπότε το θέμα θα πρέπει να αναφερθεί σε κάθε περίπτωση αμελλητί στον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ/ΔΡΟ), ώστε να διαπιστωθεί η τυχόν ανάγκη γνωστοποίησης στις αρμόδιες Αρχές.
- 2.6 Οι συνεργάτες και τυχόν τρίτα μέρη που συνεργάζονται ή επιτελούν εργασίες για λογαριασμό του Ομίλου και που έχουν ή ενδέχεται να έχουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, αναμένεται να έχουν γνώση των δικαιωμάτων που προβλέπονται σε αυτή την πολιτική, μέσω της σύναψης ειδικής πρόσθετης πράξης για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Κανένα τρίτο μέρος δεν μπορεί να έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που βρίσκονται στην κατοχή του Ομίλου, χωρίς να έχει πρώτα συνάψει συμφωνία ανάθεσης επεξεργασίας προσωπικών δεδομένων, η οποία επιβάλλει στις υποχρεώσεις του τρίτου μέρους, όχι λιγότερο επαχθείς υποχρεώσεις από εκείνες για τις οποίες έχει δεσμευθεί ο Όμιλος και παρέχει στον Όμιλο το δικαίωμα να ελέγχει τα τρίτα μέρη για τη συμμόρφωσή τους με τους όρους που περιγράφονται στη σύμβαση.

## 3. ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ (ΣΔΠΠ - PIMS)

### Δήλωση πολιτικής

- 3.1 Για να υποστηρίξει τη συμμόρφωση με το GDPR, η Διοίκηση του Ομίλου ενέκρινε και υποστήριξε την ανάπτυξη, υλοποίηση, συντήρηση και συνεχή βελτίωση ενός τεκμηριωμένου Συστήματος Διαχείρισης Προσωπικών Πληροφοριών (ΣΔΠΠ - PIMS) για τον Όμιλο.

3.2 Όλο το προσωπικό, καθώς και ορισμένα εξωτερικά τρίτα μέρη, θα λάβουν την κατάλληλη εκπαίδευση για την ορθή εφαρμογή της παρούσας πολιτικής και του ΣΔΠΠ. Οι συνέπειες της παραβίασης αυτής της πολιτικής ορίζονται στις συμβάσεις και τις συμφωνίες με τρίτους.

3.3 Κατά τον προσδιορισμό του πεδίου εφαρμογής της Πολιτικής για τη συμμόρφωση με τον Κανονισμό GDPR, ο Όμιλος λαμβάνει υπόψη:

- Τυχόν εξωτερικά και εσωτερικά ζητήματα που σχετίζονται με τον σκοπό του Ομίλου και επηρεάζουν την ικανότητά του να επιτύχει τα επιδιωκόμενα αποτελέσματα του ΣΔΠΠ.
- Τις ειδικές ανάγκες και τις προσδοκίες των ενδιαφερομένων μερών που σχετίζονται με την εφαρμογή του ΣΔΠΠ.
- Τους οργανωτικούς στόχους και υποχρεώσεις.
- Τα αποδεκτά επίπεδα κινδύνου του Ομίλου.
- Κάθε ισχύουσα νομοθετική, κανονιστική ή συμβατική υποχρέωση του Ομίλου.

3.4 Οι στόχοι του Ομίλου για συμμόρφωση με τον Κανονισμό GDPR και το ΣΔΠΠ:

- Είναι συνεπείς με αυτήν την Πολιτική.
- Είναι μετρήσιμοι.
- Λαμβάνουν υπόψη τις απαιτήσεις του Κανονισμού GDPR και τα αποτελέσματα από τις αναλύσεις κινδύνου και τα μέτρα μείωσης του κινδύνου.
- Παρακολουθούνται συνεχώς.
- Επικοινωνούνται.
- Επικαιροποιούνται κατά περίπτωση.

Ο Όμιλος τεκμηριώνει αυτούς τους στόχους στους αντίστοιχους καταγεγραμμένους στόχους συμμόρφωσης με τις απαιτήσεις του Προτύπου του GDPR και το ΣΔΠΠ.

Προκειμένου να επιτευχθούν αυτοί οι στόχοι, ο Όμιλος έχει καθορίσει:

- Τι θα γίνει.
- Ποιοι πόροι θα απαιτηθούν.
- Ποιος θα είναι υπεύθυνος.
- Πότε θα ολοκληρωθούν.
- Πώς θα αξιολογούνται τα αποτελέσματα.

#### **4. ΕΥΘΥΝΕΣ ΚΑΙ ΡΟΛΟΙ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR)**

4.1 Ο Όμιλος είναι υπεύθυνος για την επεξεργασία των δεδομένων, σύμφωνα με τον Κανονισμό GDPR.

4.2 Η Διοίκηση και όλοι όσοι κατέχουν διευθυντικό ή εποπτικό ρόλο σε όλο τον Όμιλο είναι υπεύθυνοι για την ανάπτυξη και την ενθάρρυνση ορθών διαδικασιών διαχείρισης δεδομένων προσωπικού χαρακτήρα στον Όμιλο, όσο και για το ότι οι ευθύνες καθορίζονται στις ατομικές περιγραφές θέσεων εργασίας.

4.3 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO), είναι ένας ρόλος που ορίζεται στον Κανονισμό GDPR, και δύναται να είναι, εργαζόμενος του Ομίλου και/ή εξιδεικευμένος εξωτερικός συνεργάτης ο οποίος θα αναφέρεται μέσω των εκθέσεων του σε μέλος της ανώτερης διοικητικής ομάδας του Ομίλου. για τη διαχείριση των προσωπικών δεδομένων εντός του Ομίλου όσο και για την διασφάλιση

ότι η συμμόρφωση με τη νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα και ότι η χρήση ορθών πρακτικών μπορεί να αποδεικνύεται ανά πάσα στιγμή. Οι ενέργειες που γίνονται περιλαμβάνουν:

- Την ανάπτυξη και εφαρμογή του GDPR, όπως απαιτείται από αυτή την Πολιτική.
  - Τα μέτρα ασφάλειας και τη διαχείριση κινδύνων μέσα στο πλαίσιο εφαρμογής της Πολιτικής αυτής.
- 4.4 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO), τον οποίο η Διοίκηση του Ομίλου θεωρεί ότι διαθέτει τα κατάλληλα προσόντα και την απαιτούμενη εμπειρία, έχει αναλάβει να βοηθάει για την καθημερινή τήρηση της παρούσας Πολιτικής από τον Όμιλο και, ειδικότερα, έχει αναλάβει να εξασφαλίζει ότι ο Όμιλος συμμορφώνεται με τον Κανονισμό GDPR, όπως και ότι οι Διευθυντές / Εκτελεστικά μέλη του Ομίλου στο πλαίσιο των καθημερινών τους δραστηριοτήτων, οι οποίες σχετίζονται με τη διαχείριση των δεδομένων προσωπικού χαρακτήρα στην περιοχή ευθύνης τους, συμμορφώνονται με τα προβλεπόμενα του Κανονισμού.
- 4.5 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO), έχει συγκεκριμένες ευθύνες σε σχέση με διαδικασίες, όπως οι διαδικασίες άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων και είναι το πρώτο σημείο επαφής για να αναζητήσουν οι εργαζόμενοι διευκρινίσεις σχετικά με οποιαδήποτε πτυχή της τήρησης της συμμόρφωσης με τον Κανονισμό περί της Προστασίας των Δεδομένων Προσωπικού Χαρακτήρα (GDPR).
- 4.6 Η συμμόρφωση με τη νομοθεσία περί προστασίας των δεδομένων προσωπικού χαρακτήρα είναι ευθύνη όλου του προσωπικού του Ομίλου που επιτελεί επεξεργασία προσωπικών δεδομένων.
- 4.7 Η Πολιτική Εκπαίδευσης των Εργαζομένων σε θέματα του Κανονισμού ΕΕ 2016/679 (GDPR) καθορίζει συγκεκριμένες απαιτήσεις κατάρτισης και ευαισθητοποίησης του προσωπικού σε σχέση με συγκεκριμένους επιχειρηματικούς ρόλους.
- 4.8 Τα μέλη του προσωπικού του Ομίλου είναι υπεύθυνα για τη διασφάλιση ότι τα προσωπικά δεδομένα που τους αφορούν, και τα οποία παρέχονται από τους ίδιους στον Όμιλο είναι ακριβή και ενημερωμένα.

## 5. ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Όλες οι επεξεργασίες δεδομένων προσωπικού χαρακτήρα του Ομίλου πρέπει να διεξάγονται σύμφωνα με τις αρχές προστασίας δεδομένων προσωπικού χαρακτήρα, όπως αυτές ορίζονται στο Άρθρο 5 του Κανονισμού GDPR. Οι πολιτικές και οι διαδικασίες του Ομίλου έχουν σχεδιαστεί για να διασφαλίζεται η συμμόρφωση με τις αρχές αυτές.

### 5.1 Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε νόμιμη, δίκαιη και διαφανή επεξεργασία

**Νομιμότητα** - Να αναγνωρισθεί η νόμιμη βάση πριν ξεκινήσει η επεξεργασία των προσωπικών δεδομένων. Αυτές συχνά αναφέρονται ως "συνθήκες επεξεργασίας", όπως για παράδειγμα η συγκατάθεση.

**Δικαιοσύνη** - Για να είναι δίκαιη η επεξεργασία, ο υπεύθυνος επεξεργασίας πρέπει να θέτει συγκεκριμένα στοιχεία υπόψη των υποκειμένων των δεδομένων, εφ' όσον αυτό είναι εφικτό. Αυτό ισχύει είτε τα προσωπικά δεδομένα αποκτήθηκαν απευθείας από τα πρόσωπα στα οποία αναφέρονται τα δεδομένα είτε από άλλες πηγές.

Ο Κανονισμός GDPR έχει αυξημένες απαιτήσεις σχετικά με τις πληροφορίες που πρέπει να είναι διαθέσιμες στα υποκείμενα των δεδομένων, οι οποίες καλύπτονται από την απαίτηση για «**Διαφάνεια**».

**Διαφάνεια** – Ο Κανονισμός GDPR περιλαμβάνει κανόνες για την παροχή πληροφοριών σχετικά με τα προσωπικά δεδομένα στα υποκείμενα των δεδομένων στα Άρθρα 12, 13 και 14. Αυτοί είναι λεπτομερείς



και συγκεκριμένοι, δίνοντας έμφαση στην κατανόηση και την πρόσβαση των υποκειμένων των δεδομένων στις ανακοινώσεις του Ομίλου περί απορρήτου. Οι πληροφορίες πρέπει να κοινοποιούνται στο υποκείμενο των δεδομένων σε κατανοητή μορφή με σαφή και απλή γλώσσα.

Ο Όμιλος μέσω της «Δήλωσης Απορρήτου» προβλέπει ότι συγκεκριμένες πληροφορίες πρέπει να παρέχονται στο υποκείμενο των δεδομένων:

- 5.1.1 Η ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας και, ενδεχομένως, του εκπροσώπου του.
- 5.1.2 Τα στοιχεία επικοινωνίας του Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ/DPO).
- 5.1.3 Οι σκοποί της επεξεργασίας για την οποία προορίζονται τα προσωπικά δεδομένα, καθώς και η νομική βάση της επεξεργασίας.
- 5.1.4 Η περίοδος για την οποία θα αποθηκεύονται τα προσωπικά δεδομένα.
- 5.1.5 Η παροχή δικαιώματος υποβολής αιτήματος πρόσβασης, διόρθωσης, λήθης ή διατύπωσης αντιρρήσεων για την επεξεργασία και οι προϋποθέσεις (ή η έλλειψη αυτών) σχετικά με την άσκηση αυτών των δικαιωμάτων από τα υποκείμενα των δεδομένων, όπως το αν θα επηρεαστεί η νομιμότητα προηγούμενης επεξεργασίας.
- 5.1.6 Οι κατηγορίες των σχετικών δεδομένων προσωπικού χαρακτήρα.
- 5.1.7 Οι παραλήπτες ή οι κατηγορίες παραληπτών των προσωπικών δεδομένων, κατά περίπτωση.
- 5.1.8 Όπου απαιτείται, ενημέρωση ότι ο υπεύθυνος της επεξεργασίας προτίθεται να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα και το επίπεδο προστασίας που παρέχεται στα δεδομένα προσωπικού χαρακτήρα.
- 5.1.9 Οποιοσδήποτε περαιτέρω πληροφορίες είναι απαραίτητες για να διασφαλισθεί το δικαίωμα της επεξεργασίας.

## **5.2 Τα προσωπικά δεδομένα μπορούν να συλλεχθούν μόνο για συγκεκριμένους, σαφείς και νόμιμους σκοπούς**

Τα προσωπικά δεδομένα που λαμβάνονται για συγκεκριμένο σκοπό, δεν πρέπει να χρησιμοποιούνται για σκοπό που διαφέρει από εκείνον που κοινοποιήθηκε προς το υποκείμενο των δεδομένων και επίσημα προς την Εποπτική Αρχή, μέσω των αρχείων δραστηριοτήτων επεξεργασίας του Άρθρου 30 του Κανονισμού GDPR.

## **5.3 Τα προσωπικά δεδομένα πρέπει να είναι επαρκή, συναφή και να περιορίζονται σε ό,τι είναι απαραίτητο για την επεξεργασία**

- 5.3.1 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) μεριμνά για τη διασφάλιση ότι ο Όμιλος δεν συλλέγει πληροφορίες που δεν είναι απολύτως απαραίτητες για τον σκοπό για τον οποίο αποκτήθηκαν.
- 5.3.2 Όλα τα έντυπα συλλογής δεδομένων (σε ηλεκτρονική ή έγχαρτη μορφή), συμπεριλαμβανομένων των απαιτήσεων για συλλογή δεδομένων μέσω νέων συστημάτων πληροφοριών, πρέπει να περιλαμβάνουν μια δήλωση δίκαιης επεξεργασίας ή να παρέχεται ο σύνδεσμος με τη δήλωση προστασίας προσωπικών δεδομένων και να εγκρίνονται από τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ/DPO).
- 5.3.3 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) θα προτείνει, με την αναφορά του προς την Διοίκηση του Ομίλου, περιοχές προς εξέταση από τον εσωτερικό έλεγχο, για να διασφαλιστεί ότι τα συλλεγόμενα δεδομένα εξακολουθούν να είναι επαρκή, συναφή και όχι υπερβάλλοντα.

#### **5.4 Τα προσωπικά δεδομένα πρέπει να είναι ακριβή και ενημερωμένα και να γίνεται προσπάθεια να διαγράφονται ή να διορθώνονται χωρίς καθυστέρηση**

- 5.4.1 Τα δεδομένα που αποθηκεύονται από τον υπεύθυνο επεξεργασίας πρέπει να αναθεωρούνται και να ενημερώνονται ανάλογα με τις ανάγκες. Δεν πρέπει να διατηρούνται δεδομένα εκτός αν είναι εύλογη η υπόθεση ότι αυτά είναι ακριβή.
- 5.4.2 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) είναι υπεύθυνος για την διασφάλιση ότι όλο το προσωπικό εκπαιδεύεται σχετικά με τη σημασία της συλλογής επακριβών δεδομένων και την διατήρησή τους.
- 5.4.3 Είναι επίσης ευθύνη του υποκειμένου των δεδομένων να διασφαλίζει ότι τα δεδομένα που βρίσκονται στην κατοχή του Ομίλου είναι ακριβή και ενημερωμένα. Η συμπλήρωση ενός εντύπου εγγραφής ή φόρμας αίτησης από το υποκείμενο των δεδομένων θα περιλαμβάνει δήλωση ότι τα δεδομένα που περιέχονται σε αυτήν είναι ακριβή κατά την ημερομηνία υποβολής.
- 5.4.4 Οι υπάλληλοι, το προσωπικό, οι πελάτες, οι συνεργάτες και οι τρίτοι έχουν την ευθύνη να κοινοποιούν στον Όμιλο τυχόν αλλαγές στα δεδομένα που τους αφορούν, ώστε να είναι δυνατή η ενημέρωση των προσωπικών τους δεδομένων που διατηρεί ο Όμιλος. Είναι ευθύνη του Ομίλου να διασφαλιστεί ότι η κοινοποίηση σχετικά με την αλλαγή των προσωπικών δεδομένων καταγράφεται και η επεξεργασία γίνεται στα νέα επικαιροποιημένα δεδομένα.
- 5.4.5 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) είναι υπεύθυνος για τη διασφάλιση της θέσπισης κατάλληλων πολιτικών και διαδικασιών για την διατήρηση της ακρίβειας των δεδομένων και την συνεχή ενημέρωσή τους, λαμβάνοντας υπόψη τον όγκο των δεδομένων που συλλέγονται, την ταχύτητα με την οποία αυτά μπορεί να αλλάξουν και τυχόν άλλους σχετικούς παράγοντες.
- 5.4.6 Τουλάχιστον σε διετή βάση, ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) θα επανεξετάζει τις ημερομηνίες διακράτησης όλων των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία από τον Όμιλο, τα οποία διατηρούνται στο αρχείο δραστηριοτήτων επεξεργασίας, και θα εντοπίζει όλα τα δεδομένα που δεν απαιτούνται πλέον στο πλαίσιο του καταγεγραμμένου σκοπού επεξεργασίας και θα υποβάλει προτάσεις προς την Διοίκηση του Ομίλου. Αυτά τα δεδομένα θα διαγράφονται με ασφάλεια σύμφωνα με την Πολιτική Διατήρησης & Καταστροφής Αρχείων.
- 5.4.7 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) είναι υπεύθυνος για την απάντηση σε αιτήματα για διόρθωση που υποβάλλονται από τα υποκείμενα των δεδομένων, εντός ενός μηνός από την υποβολή του αιτήματος. Το διάστημα αυτό μπορεί να επεκταθεί κατά δύο επιπλέον μήνες για περίπλοκα αιτήματα. Εάν ο Όμιλος αποφασίσει να μην συμμορφωθεί με το αίτημα, ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) πρέπει να απαντήσει στα υποκείμενα των δεδομένων για να εξηγήσει το σκεπτικό της απόφασης και να ενημερώσει για το δικαίωμά τους να διαμαρτυρηθούν προς την εποπτική αρχή ή και να καταφύγουν σε δικαστική προσφυγή.
- 5.4.8 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) είναι υπεύθυνος για τη λήψη των κατάλληλων μέτρων ώστε, εάν έχουν διαβιβαστεί ανακριβή ή παρωχημένα δεδομένα προσωπικού χαρακτήρα σε τρίτους, αυτοί να ενημερωθούν ότι οι πληροφορίες είναι ανακριβείς ή / και παρωχημένες και δεν πρέπει να χρησιμοποιούνται για τη λήψη αποφάσεων σχετικά με τα συγκεκριμένα υποκείμενα των δεδομένων, όπως και για τη διαβίβαση οποιασδήποτε διόρθωσης επί των προσωπικών δεδομένων σε τρίτα μέρη όπου αυτό απαιτείται.

#### **5.5 Τα δεδομένα προσωπικού χαρακτήρα πρέπει να τηρούνται με τέτοιο τρόπο ώστε το υποκείμενο των δεδομένων να μπορεί να ταυτοποιηθεί μόνον εφόσον αυτό είναι αναγκαίο για την επεξεργασία**

- 5.5.1 Όταν τα προσωπικά δεδομένα διατηρούνται πέρα από την ημερομηνία επεξεργασίας, θα [ελαχιστοποιούνται/ κρυπτογραφούνται / ψευδωνυμοποιούνται] προκειμένου να προστατευτεί η

ταυτότητα του προσώπου στο οποίο αναφέρονται τα δεδομένα σε περίπτωση παραβίασης των δεδομένων.

- 5.5.2 Τα προσωπικά δεδομένα θα διατηρούνται σύμφωνα με την Πολιτική Διατήρησης & Καταστροφής Αρχείων και, μόλις περατωθεί η ημερομηνία διακράτησής τους, θα πρέπει να καταστρέφονται με ασφάλεια σύμφωνα με την Πολιτική αυτή.
- 5.5.3 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) πρέπει να εγκρίνει ρητά κάθε διατήρηση δεδομένων που υπερβαίνει τις περιόδους διακράτησης που ορίζονται στο αρχείο των δραστηριοτήτων επεξεργασίας του Ομίλου, και πρέπει να διασφαλίζεται ότι η αιτιολογία είναι σαφώς προσδιορισμένη και σύμφωνη με τις απαιτήσεις της νομοθεσίας για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η έγκριση δε αυτή θα πρέπει να είναι καταγεγραμμένη.

## **5.6 Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να διασφαλίζεται η απαραίτητη ασφάλεια**

Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) θα προβεί σε Αξιολόγηση του Κινδύνου, λαμβάνοντας υπόψη το πλαίσιο των διαδικασιών επεξεργασίας του Ομίλου και όλα τα εφαρμοζόμενα μέτρα προστασίας.

Για τον προσδιορισμό της καταλληλότητας των μέτρων προστασίας, ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) θα πρέπει επίσης να εξετάσει την έκταση της πιθανής ζημίας ή απώλειας που μπορεί να προκληθεί στα φυσικά πρόσωπα (π.χ. μέλη του προσωπικού, πελάτες ή προμηθευτές) σε περίπτωση παραβίασης της ασφάλειας, καθώς και τυχόν επίπτωση στη φήμη του Ομίλου, συμπεριλαμβανομένης της πιθανής απώλειας εμπιστοσύνης εκ μέρους των πελατών.

Κατά την αξιολόγηση των κατάλληλων τεχνικών μέτρων, ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) σε συνεργασία με τον Υπεύθυνο Ασφαλείας Πληροφοριακών Συστημάτων του Ομίλου θα εξετάσει τα εξής:

- Προστασία με κωδικό πρόσβασης.
- Αυτόματο κλείδωμα υπολογιστών.
- Κατάργηση δικαιωμάτων πρόσβασης σε USB και άλλα αποθηκευτικά μέσα μνήμης.
- Χρήση λογισμικού προστασίας από ιούς και χρήση τειχών προστασίας (Firewalls).
- Δικαιώματα πρόσβασης στο δίκτυο του Ομίλου βάσει ρόλων, συμπεριλαμβανομένων εκείνων που εκχωρούνται σε έκτακτο προσωπικό.
- Κρυπτογράφηση συσκευών που εγκαταλείπουν τις εγκαταστάσεις του Ομίλου, όπως φορητοί υπολογιστές, USB media, κ.λπ..
- Ασφάλεια Τοπικών και Ευρυζωνικών Δικτύων.
- Χρήση Τεχνολογικών μεθόδων για την προστασία της ιδιωτικότητας, όπως η ψευδωνυμοποίηση και η ανωνυμοποίηση.
- Προσδιορισμός κατάλληλων διεθνών προτύπων ασφαλείας που εφαρμόζει ο Όμιλος.

Κατά την αξιολόγηση των κατάλληλων οργανωτικών μέτρων, ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) θα εξετάσει τα εξής:

- Την απαραίτητη εκπαίδευση για την προστασία των δεδομένων προσωπικού χαρακτήρα προς όλα τα μέλη του προσωπικού του Ομίλου.
- Μέτρα που πιστοποιούν την αξιοπιστία των εργαζομένων (όπως αναφορές προηγούμενης εργασίας, συστατικές επιστολές, κ.λπ.).

- Τη συμπερίληψη της προστασίας των δεδομένων στις συμβάσεις εργασίας.
- Προσδιορισμό των μέτρων πειθαρχικής δράσης για παραβιάσεις δεδομένων προσωπικού χαρακτήρα.
- Παρακολούθηση της συμμόρφωσης του προσωπικού με τα σχετικά πρότυπα Ασφάλειας.
- Έλεγχοι φυσικής και λογικής πρόσβασης σε ηλεκτρονικά και φυσικά αρχεία.
- Υιοθέτηση σαφούς πολιτικής «καθαρού γραφείου».
- Αποθήκευση έγχαρτων δεδομένων σε αντιπυρικούς φοριαμούς που κλειδώνουν.
- Περιορισμός της χρήσης φορητών ηλεκτρονικών συσκευών εκτός του χώρου εργασίας.
- Περιορισμός της χρήσης των προσωπικών συσκευών του εργαζομένου για χρήση εντός του χώρου εργασίας.
- Υιοθέτηση σαφών κανόνων σχετικά με τους κωδικούς πρόσβασης.
- Δημιουργία τακτικών αντιγράφων ασφαλείας των προσωπικών δεδομένων και αποθήκευση των μέσων σε εναλλακτικό απομακρυσμένο χώρο.
- Επιβολή συμβατικών υποχρεώσεων στους οργανισμούς - παραλήπτες των δεδομένων προσωπικού χαρακτήρα, ώστε να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας κατά τη μεταφορά δεδομένων εκτός του χώρου της ΕΕ.

Αυτά τα μέτρα προστασίας έχουν επιλεγεί με βάση τους κινδύνους που προσδιορίστηκαν για τα προσωπικά δεδομένα και τις πιθανότητες βλάβης ή κινδύνου για τα φυσικά πρόσωπα τα δεδομένα των οποίων υπόκεινται σε επεξεργασία.

Η συμμόρφωση του Ομίλου με αυτή την αρχή περιέχεται στο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), το οποίο έχει αναπτυχθεί σύμφωνα με το ISO / IEC 27001: 2013 και την πολιτική ασφάλειας των πληροφοριών που περιγράφεται στην Πολιτική Αποδεκτής και Ασφαλούς Χρήσης των Συστημάτων και Πόρων Πληροφορικής & Τηλεπικοινωνιών (Information Security Policy).

### **5.7 Ο υπεύθυνος της επεξεργασίας πρέπει να είναι σε θέση να αποδεικνύει τη συμμόρφωση με τις υπόλοιπες αρχές του GDPR (Αρχή της Λογοδοσίας)**

Το GDPR περιλαμβάνει διατάξεις που προωθούν την υπευθυνότητα και τη διακυβέρνηση των δεδομένων προσωπικού χαρακτήρα. Αυτές συμπληρώνουν τις απαιτήσεις διαφάνειας του Κανονισμού GDPR. Συμμορφούμενος ο Όμιλος με την αρχή της Λογοδοσίας, όπως αυτή αναφέρεται στο άρθρο 5 παράγραφος 2 του Κανονισμού, είναι σε θέση να αποδεικνύει ότι συμμορφώνεται με τις αρχές αυτές και δηλώνει ρητά ότι αναλαμβάνει την ευθύνη.

Ο Όμιλος θα αποδεικνύει ότι συμμορφώνεται με τις αρχές προστασίας των δεδομένων προσωπικού χαρακτήρα με την εφαρμογή πολιτικών για την προστασία των δεδομένων, θεσπίζοντας και ακολουθώντας κώδικες δεοντολογίας, εφαρμόζοντας Οργανωτικά και Τεχνικά μέτρα προστασίας, καθώς και την υιοθέτηση τεχνικών όπως η προστασία των δεδομένων από τον σχεδιασμό, διεξαγωγή ασκήσεων «Εκτίμησης Επιπτώσεων της Προστασίας Δεδομένων (ΕΕΠΔ)», διαδικασίες κοινοποίησης παραβίασης δεδομένων προς την εποπτική αρχή και ύπαρξης σχεδίων αντιμετώπισης περιστατικών ασφαλείας.

## **6. ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ**

### **6.1 Τα υποκείμενα των δεδομένων έχουν τα ακόλουθα δικαιώματα όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που έχει στη κατοχή του ο Όμιλος**

- 6.1.1 Να υποβάλουν αίτημα πρόσβασης για θέματα σχετικά με τη φύση των δεδομένων προσωπικού χαρακτήρα που ο Όμιλος έχει στη κατοχή του και γνωστοποίηση των προσώπων στα οποία τα δεδομένα αυτά έχουν τυχόν διαβιβασθεί.
- 6.1.2 Να αποφεύγεται επεξεργασία που μπορεί να προκαλέσει πιθανή ζημιά για τα υποκείμενα των δεδομένων.
- 6.1.3 Να εμποδίζεται η επεξεργασία για σκοπούς άμεσου μάρκετινγκ (προώθηση προϊόντος), χωρίς την λήψη σχετικής συναίνεσης.
- 6.1.4 Να ενημερωθούν για τυχόν μηχανισμούς αυτοματοποιημένης διαδικασίας λήψης αποφάσεων που θα τους επηρεάσει σημαντικά.
- 6.1.5 Να διεκδικήσουν αποζημίωση εάν υποστούν ζημιά από οποιαδήποτε παράβαση του Κανονισμού GDPR.
- 6.1.6 Να ασκήσουν το δικαίωμά τους για τη διόρθωση, την απαγόρευση, τη διαγραφή, συμπεριλαμβανομένου του δικαιώματος στη λήθη ή καταστροφής ανακριβών δεδομένων.
- 6.1.7 Να ζητήσουν από την Εποπτική Αρχή να εκτιμήσει εάν έχει παραβιαστεί οποιαδήποτε διάταξη του Κανονισμού GDPR από τον υπεύθυνο της επεξεργασίας.
- 6.1.8 Να τους παρασχεθούν τα προσωπικά τους δεδομένα σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από λογισμικό, καθώς και το δικαίωμα να διαβιβασθούν τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα.
- 6.1.9 Να αντιτάσσονται σε οποιοδήποτε αυτοματοποιημένο προφίλ που τους αφορά και το οποίο έχει δημιουργηθεί χωρίς συγκατάθεση.

## **6.2 Ο Όμιλος διασφαλίζει ότι τα υποκείμενα των δεδομένων μπορούν να ασκούν τα δικαιώματα**

- 6.2.1 Να υποβάλλουν αίτημα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που τους αφορούν, όπως περιγράφεται στην αντίστοιχη διαδικασία. Ο Όμιλος δεσμεύεται να αποκρίνεται στα αιτήματα πρόσβασης των υποκειμένων των δεδομένων σύμφωνα με όσα προβλέπονται στον Κανονισμό GDPR.
- 6.2.2 Να υποβάλλουν καταγγελίες σχετικά με την επεξεργασία των προσωπικών τους δεδομένων.

## **7. ΣΥΓΚΑΤΑΘΕΣΗ**

- 7.1 Ο Όμιλος κατανοεί την έννοια της «συγκατάθεσης» που σημαίνει ότι η συγκατάθεση του υποκειμένου των δεδομένων έχει δοθεί ρητά και ελεύθερα και αποτελεί μια συγκεκριμένη, ενημερωμένη και σαφή ένδειξη των επιθυμιών του υποκειμένου των δεδομένων ότι με δήλωσή του ή με σαφή καταφατική ενέργεια, συμφωνεί με την επεξεργασία των προσωπικών δεδομένων που το αφορούν. Το υποκείμενο των δεδομένων μπορεί να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή.
- 7.2 Ο Όμιλος κατανοεί την έννοια της «συγκατάθεσης» που σημαίνει ότι το πρόσωπο στο οποίο αναφέρονται τα δεδομένα προσωπικού χαρακτήρα έχει ενημερωθεί πλήρως για την προβλεπόμενη επεξεργασία και έχει υποδηλώσει τη συμφωνία του, ενώ έχει τη δυνατότητα να το πράξει χωρίς να του ασκούνται πιέσεις. Η συγκατάθεση που αποκτάται υπό πίεση ή βάσει παραπλανητικών πληροφοριών δεν αποτελεί έγκυρη βάση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

- 7.3 Πρέπει να υπάρξει κάποια ενεργή επικοινωνία μεταξύ των μερών για να αποδεικνύεται η ενεργός συγκατάθεση. Η συγκατάθεση δεν μπορεί να συναχθεί από τη μη απάντηση σε μια επικοινωνία. Ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι έχει ληφθεί η συγκατάθεση του υποκειμένου των δεδομένων για τη διαδικασία της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.
- 7.4 Όσον αφορά ευαίσθητα δεδομένα προσωπικού χαρακτήρα του Άρθρου 9, πρέπει να ληφθεί η ρητή γραπτή συγκατάθεση των υποκειμένων των δεδομένων, εκτός εάν υπάρχει άλλη νομική βάση για την επεξεργασία.
- 7.5 Στις περισσότερες περιπτώσεις, η συγκατάθεση για την επεξεργασία των προσωπικών και ευαίσθητων δεδομένων προσωπικού χαρακτήρα επιτυγχάνεται συνήθως με τη χρήση τυποποιημένων εγγράφων συγκατάθεσης του Ομίλου, «Πρόσθετη Πράξη Ανάθεσης Επεξεργασίας Προσωπικών Δεδομένων» ή «Δήλωση Απορρήτου», π.χ. όταν ένας νέος πελάτης υπογράφει μια σύμβαση, ή κατά την εισδοχή ενός φυσικού προσώπου σε διάφορα προγράμματα.
- 7.6 Όπου ο Όμιλος παρέχει ηλεκτρονικές υπηρεσίες σε παιδιά, πρέπει να λαμβάνεται η γονική συγκατάθεση ή η συγκατάθεση του νόμιμου κηδεμόνα. Η απαίτηση αυτή ισχύει για παιδιά ηλικίας κάτω των 16 ετών (εκτός εάν το κράτος μέλος έχει προβλέψει χαμηλότερο όριο ηλικίας, το οποίο όμως δεν μπορεί να είναι κατώτερο από 13).

## 8. ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

- 8.1 Όλα τα μέλη του προσωπικού του Ομίλου είναι υπεύθυνα για την διασφάλιση ότι όλα τα δεδομένα προσωπικού χαρακτήρα που ο Όμιλος έχει στην κατοχή του και τα οποία τα αφορούν, διατηρούνται με ασφάλεια και δεν αποκαλύπτονται κάτω από οποιοσδήποτε συνθήκες σε οποιονδήποτε τρίτο, εκτός αν ο τρίτος έχει ειδικά εξουσιοδοτηθεί από τον Όμιλο ότι δύναται να λαμβάνει τέτοιες πληροφορίες και έχει συνάψει αντίστοιχη συμφωνία εμπιστευτικότητας.
- 8.2 Πρόσβαση στα δεδομένα προσωπικού χαρακτήρα θα δίδεται μόνο σε όσους έχουν σχετική εξουσιοδότηση, βάσει των καθηκόντων τους. Όλα τα προσωπικά δεδομένα θα πρέπει να αντιμετωπίζονται με την υψηλότερη ασφάλεια και πρέπει ενδεικτικά να τηρούνται:
  - σε κλειδωμένο δωμάτιο με ελεγχόμενη πρόσβαση, ή/και
  - σε ένα συρτάρι με κλειδαριά ή σε πυρασφαλή φοριαμό με κλειδαριά, ή/και
  - εάν είναι σε ηλεκτρονική μορφή, προστατεύονται με κωδικό πρόσβασης, ή/και
  - αποθηκευμένα με κρυπτογράφηση σε ηλεκτρονικά μέσα.
- 8.3 Πρέπει να ληφθεί μέριμνα, ώστε οι θρόνες και οι τερματικοί σταθμοί των υπολογιστών να μην είναι ορατοί, εκτός από τους εξουσιοδοτημένους υπαλλήλους και τα μέλη του προσωπικού του Ομίλου. Όλα τα μέλη του προσωπικού καλούνται να υπογράψουν την Πολιτική Αποδεκτής και Ασφαλούς Χρήσης των Συστημάτων και Πόρων Πληροφορικής & Τηλεπικοινωνιών (Information Security Policy), προτού τους δοθεί πρόσβαση σε εταιρικές πληροφορίες οποιουδήποτε είδους, η οποία περιγράφει λεπτομερώς τους κανόνες σχετικά με τα χρονικά διαστήματα κλειδώματος της οθόνης των τερματικών.
- 8.4 Οι μη ηλεκτρονικές εγγραφές δεδομένων προσωπικού χαρακτήρα δεν επιτρέπεται να παραμένουν εκεί όπου μπορούν να γίνουν προσβάσιμες από μη εξουσιοδοτημένα μέλη του προσωπικού και δεν μπορούν να απομακρυνθούν από τις εγκαταστάσεις του Ομίλου χωρίς την ανάλογη εξουσιοδότηση. Όταν τα φυσικά αρχεία δεν απαιτούνται πλέον θα πρέπει να διαγράφονται από την ασφαλή φύλαξη, σύμφωνα με την Πολιτική Διατήρησης & Καταστροφής Αρχείων.
- 8.5 Τα δεδομένα προσωπικού χαρακτήρα μπορούν να διαγράφονται ή να καταστρέφονται σύμφωνα με την Πολιτική Διατήρησης & Καταστροφής Αρχείων. Τα φυσικά αρχεία που έχουν φθάσει την

ημερομηνία διακράτησής τους πρέπει να καταστρέφονται σύμφωνα με την Πολιτική Διατήρησης & Καταστροφής Αρχείων. Οι σκληροί δίσκοι των αποσυρόμενων υπολογιστών πρέπει να αφαιρούνται και να διαγράφονται τα δεδομένα τους με ασφαλή τρόπο πριν από την διάθεσή τους.

- 8.6 Η απομακρυσμένη επεξεργασία δεδομένων προσωπικού χαρακτήρα παρουσιάζει δυνητικά μεγαλύτερο κίνδυνο απώλειας, κλοπής ή ζημίας για τα δεδομένα προσωπικού χαρακτήρα. Τα μέλη του προσωπικού πρέπει να έχουν ειδική εξουσιοδότηση για την επεξεργασία των δεδομένων εκτός των εγκαταστάσεων του Ομίλου.

## 9. ΓΝΩΣΤΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ

- 9.1 Ο Όμιλος διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα δεν αποκαλύπτονται σε μη εξουσιοδοτημένους τρίτους, συμπεριλαμβανομένων μελών της οικογένειας, φίλων, κυβερνητικών οργάνων και, σε ορισμένες περιπτώσεις, της αστυνομίας. Όλα τα μέλη του προσωπικού του Ομίλου θα πρέπει να είναι πολύ προσεκτικά όταν καλούνται να αποκαλύψουν δεδομένα προσωπικού χαρακτήρα για κάποιο φυσικό πρόσωπο σε τρίτους. Είναι σημαντικό να υπάρχει κατά νου κατά πόσον η γνωστοποίηση των πληροφοριών αυτών είναι σχετική και απαραίτητη για τη διεξαγωγή των δραστηριοτήτων του Ομίλου.
- 9.2 Όλες οι αιτήσεις γνωστοποίησης δεδομένων για έναν από τους ανωτέρω λόγους πρέπει να συνοδεύονται από τις απαραίτητες αιτήσεις και όλες αυτές οι γνωστοποιήσεις πρέπει να είναι στη διάθεση του Υπευθύνου Προστασίας Δεδομένων (ΥΠΑ/DPO) του Ομίλου.

## 10. ΔΙΑΤΗΡΗΣΗ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

- 10.1 Ο Όμιλος δεν φυλάσσει τα δεδομένα προσωπικού χαρακτήρα υπό μορφή που να επιτρέπει την αναγνώριση των προσώπων, στα οποία αναφέρονται τα δεδομένα, και για χρονικό διάστημα μεγαλύτερο από αυτό που είναι αναγκαίο σε σχέση με τους σκοπούς για τους οποίους αρχικά συλλέχθηκαν τα δεδομένα.
- 10.2 Ο Όμιλος μπορεί να αποθηκεύει τα δεδομένα προσωπικού χαρακτήρα για μεγαλύτερο χρονικό διάστημα από το όριο διακράτησης εάν τα δεδομένα προσωπικού χαρακτήρα πρόκειται να υποβληθούν σε επεξεργασία αποκλειστικά για λόγους αρχειοθέτησης, για λόγους δημόσιου συμφέροντος, για λόγους επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, με την επιφύλαξη της εφαρμογής κατάλληλων τεχνικών και οργανωτικών μέτρων για τη διασφάλιση των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων.
- 10.3 Η περίοδος διακράτησης για κάθε κατηγορία δεδομένων προσωπικού χαρακτήρα καθορίζεται στην Πολιτική Διατήρησης & Καταστροφής Αρχείων μαζί με τα κριτήρια που χρησιμοποιούνται για τον προσδιορισμό αυτής της περιόδου, συμπεριλαμβανομένων τυχόν νομικών και κανονιστικών υποχρεώσεων του Ομίλου για τη διατήρηση των δεδομένων για αντίστοιχο χρονικό διάστημα.
- 10.4 Η Πολιτική Διατήρησης & Καταστροφής Αρχείων των δεδομένων προσωπικού χαρακτήρα του Ομίλου θα πρέπει να τηρείται σε όλες τις περιστάσεις.
- 10.5 Τα προσωπικά δεδομένα πρέπει να καταστρέφονται με ασφάλεια σύμφωνα με τον Κανονισμό GDPR – τα δεδομένα προσωπικού χαρακτήρα πρέπει να τυγχάνουν της επεξεργασίας με τον κατάλληλο τρόπο, ώστε να διατηρείται η ασφάλεια, προστατεύοντας έτσι τα "δικαιώματα και τις ελευθερίες" των υποκειμένων των δεδομένων. Κάθε καταστροφή των προσωπικών δεδομένων θα γίνεται σύμφωνα με την Πολιτική Διατήρησης & Καταστροφής Αρχείων.

## 11. ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ

11.1 Όλες οι μεταφορές δεδομένων από χώρες της ΕΕ προς χώρες εκτός ΕΕ (που αναφέρονται στον Κανονισμό GDPR ως «τρίτες χώρες») είναι παράνομες, εκτός εάν υπάρχει κατάλληλο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων των υποκειμένων των δεδομένων.

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα εκτός της ΕΕ απαγορεύεται εκτός εάν ισχύουν μία ή περισσότερες από τις καθορισμένες διασφαλίσεις ή εξαιρέσεις:

### 11.1.1 Απόφαση επάρκειας

Η Ευρωπαϊκή Επιτροπή μπορεί και αξιολογεί τρίτες χώρες, περιοχές ή / και ειδικούς τομείς εντός των τρίτων χωρών, προκειμένου να αποφανθεί εάν υπάρχει σε αυτές το κατάλληλο επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων. Σε αυτές τις περιπτώσεις δεν απαιτείται έγκριση για τη μεταφορά δεδομένων προσωπικού χαρακτήρα.

Οι χώρες που είναι μέλη του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ), αλλά όχι της ΕΕ, γίνονται δεκτές ότι πληρούν τις προϋποθέσεις για μια απόφαση επάρκειας.

Κατάλογος των χωρών που ανταποκρίνονται σήμερα στις απαιτήσεις επάρκειας της Επιτροπής δημοσιεύονται στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.  
[http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

### 11.1.2 Ασπίδα προστασίας προσωπικών δεδομένων

Εάν ο Όμιλος επιθυμεί να μεταφέρει δεδομένα προσωπικού χαρακτήρα από την ΕΕ σε έναν οργανισμό στις Ηνωμένες Πολιτείες, θα πρέπει προηγουμένως να ελέγξει ότι ο οργανισμός έχει εγγραφεί στο Privacy Shield του Υπουργείου Εμπορίου των ΗΠΑ. Οι υποχρεώσεις που ισχύουν για τις εταιρείες βάσει του Privacy Shield περιλαμβάνονται στις «Αρχές Προστασίας Προσωπικών Δεδομένων». Το Υπουργείο Εμπορίου των ΗΠΑ είναι υπεύθυνο για τη διαχείριση και την ασπίδα προστασίας προσωπικών δεδομένων διασφαλίζοντας ότι οι εταιρείες θα ανταποκριθούν στις δεσμεύσεις τους. Προκειμένου να είναι σε θέση να πάρουν τη σχετική πιστοποίηση, οι εταιρείες πρέπει να έχουν μια πολιτική απορρήτου σύμφωνα με τις αρχές περί προστασίας της ιδιωτικότητας, π.χ. τη χρήση, την αποθήκευση και την περαιτέρω μεταφορά των προσωπικών δεδομένων σύμφωνα με ένα ικανό σύνολο κανόνων προστασίας δεδομένων και μέτρων ασφαλείας. Η προστασία που παρέχεται στα δεδομένα προσωπικού χαρακτήρα ισχύει ανεξάρτητα από το εάν τα προσωπικά δεδομένα αφορούν κατοίκους της ΕΕ ή όχι. Οι οργανισμοί πρέπει να ανανεώνουν την "ιδιότητα μέλους" τους στην Ασπίδα Προστασίας Προσωπικών Δεδομένων σε ετήσια βάση. Εάν δεν το κάνουν, δεν μπορούν πλέον να λαμβάνουν και να χρησιμοποιούν προσωπικά δεδομένα προερχόμενα από την ΕΕ μέσα σ' αυτό το πλαίσιο.

#### Αξιολόγηση της επάρκειας από τον υπεύθυνο επεξεργασίας δεδομένων

Κατά την αξιολόγηση της επάρκειας του παραλήπτη των δεδομένων, ο υπεύθυνος της επεξεργασίας ο οποίος μεταφέρει δεδομένα προσωπικού χαρακτήρα εκτός ΕΕ, πρέπει να λάβει υπόψη τους ακόλουθους παράγοντες:

- τη φύση των πληροφοριών που μεταφέρονται,
- τη χώρα ή την περιοχή προέλευσης και τον τελικό προορισμό των δεδομένων προσωπικού χαρακτήρα,
- πώς θα χρησιμοποιηθούν τα προσωπικά δεδομένα και για πόσο καιρό,
- τους νόμους και τις πρακτικές της χώρας του παραλήπτη των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των σχετικών κωδίκων δεοντολογίας και των διεθνών υποχρεώσεων, και
- τα μέτρα ασφαλείας που πρέπει να ληφθούν όσον αφορά τα προσωπικά δεδομένα που μεταφέρονται στο εξωτερικό.



### 11.1.3 Δεσμευτικοί Εταιρικοί Κανόνες

Ο Όμιλος δύναται να χρησιμοποιεί εγκεκριμένους δεσμευτικούς εταιρικούς κανόνες για τη μεταφορά δεδομένων εκτός ΕΟΧ. Αυτό απαιτεί την προηγούμενη υποβολή στην αρμόδια εποπτική αρχή προς έγκριση των κανόνων που ο Όμιλος πρόκειται να επικαλεστεί.

### 11.1.4 Πρότυπες Ρήτρες Συμβάσεων

Ο Όμιλος μπορεί να υιοθετεί εγκεκριμένες πρότυπες συμβατικές ρήτρες για τη διαβίβαση δεδομένων εκτός του ΕΟΧ. Εάν ο Όμιλος υιοθετήσει τις πρότυπες συμβατικές ρήτρες που έχουν εγκριθεί από την αρμόδια εποπτική αρχή, υπάρχει αυτόματη αναγνώριση της επάρκειας.

### 11.1.5 Εξαιρέσεις

Εφόσον δεν υπάρχει απόφαση επάρκειας ή η ιδιότητα του μέλους του Privacy Shield, ή/και δεσμευτικοί εταιρικοί κανόνες, ή / και οι πρότυπες συμβατικές ρήτρες, η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, πραγματοποιείται μόνο με την προϋπόθεση ενός από τους παρακάτω όρους:

- το πρόσωπο, στο οποίο αναφέρονται τα δεδομένα, έχει συναινέσει ρητά στην προτεινόμενη μεταφορά αφού πρώτα έχει ενημερωθεί σχετικά για τους ενδεχόμενους κινδύνους αυτών των μεταφορών για το υποκείμενο των δεδομένων, λόγω της έλλειψης απόφασης επάρκειας και των κατάλληλων διασφαλίσεων,
- η μεταφορά είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου της επεξεργασίας ή για την εφαρμογή των προ-συμβατικών μέτρων που λαμβάνονται κατόπιν αιτήματος του προσώπου στο οποίο αναφέρονται τα δεδομένα,
- η μεταφορά είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης που συνάπτεται προς το συμφέρον του υποκειμένου των δεδομένων μεταξύ του υπεύθυνου επεξεργασίας και άλλου φυσικού ή νομικού προσώπου,
- η μεταφορά είναι απαραίτητη για σημαντικούς λόγους δημοσίου συμφέροντος,
- η μεταφορά είναι απαραίτητη για τη σύσταση, άσκηση ή υπεράσπιση νομικών απαιτήσεων, ή/και
- η μεταφορά είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του προσώπου, στο οποίο αναφέρονται τα δεδομένα ή άλλων προσώπων, όταν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είναι φυσικά ή νομικά ανίκανο να δώσει τη συγκατάθεσή του.

## 12. ΜΗΤΡΩΟ ΠΟΡΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ / ΑΠΟΓΡΑΦΗ ΔΕΔΟΜΕΝΩΝ

12.1 Ο Όμιλος έχει καθιερώσει μια διαδικασία καταγραφής και αποτύπωσης της ροής των δεδομένων προσωπικού χαρακτήρα στο Αρχείο Δραστηριοτήτων Επεξεργασίας, ως μέρος της προσέγγισής του για την αντιμετώπιση των κινδύνων και των ευκαιριών στο πλαίσιο του έργου συμμόρφωσης με τον Κανονισμό GDPR.

Το Αρχείο Δραστηριοτήτων Επεξεργασίας, όπου καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και η ροή τους περιλαμβάνει:

- Τις επιχειρηματικές δραστηριότητες που χρησιμοποιούν προσωπικά δεδομένα.
- Την πηγή προέλευσης των δεδομένων προσωπικού χαρακτήρα.
- Τον αριθμό των υποκειμένων των δεδομένων στα οποία αναφέρονται τα δεδομένα.
- Περιγραφή κάθε στοιχείου των προσωπικών δεδομένων.

- Την δραστηριότητα επεξεργασίας.
  - Τις κατηγορίες των προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία.
  - Τεκμηρίωση του σκοπού για τον οποίο χρησιμοποιείται κάθε κατηγορία δεδομένων προσωπικού χαρακτήρα.
  - Καταγραφή των παραληπτών και δυνητικών παραληπτών των προσωπικών δεδομένων.
  - Αποτύπωση του ρόλου του Ομίλου σε όλη τη ροή δεδομένων.
  - Τα βασικά συστήματα και τους χώρους αποθήκευσης των δεδομένων.
  - Οποιαδήποτε πληροφορία για τη μεταφορά δεδομένων.
  - Όλες τις απαιτήσεις διακράτησης και διαγραφής των δεδομένων προσωπικού χαρακτήρα.
- 12.2 Ο Όμιλος έχει επίγνωση των κινδύνων που συνδέονται με την επεξεργασία συγκεκριμένων τύπων προσωπικών δεδομένων.
- 12.2.1 Ο Όμιλος αξιολογεί το επίπεδο κινδύνου για τα φυσικά πρόσωπα που σχετίζεται με την επεξεργασία των προσωπικών τους δεδομένων. Οι Εκτιμήσεις Επιπτώσεων της Προστασίας Δεδομένων (ΕΕΠΔ) διεξάγονται σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον ίδιο τον Όμιλο, αλλά και σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από τρίτους οργανισμούς για λογαριασμό του Ομίλου.
- 12.2.2 Ο Όμιλος θα διαχειρίζεται τους κινδύνους που εντοπίζονται από την ανάλυση κινδύνου, προκειμένου να μειωθεί η πιθανότητα μη συμμόρφωσης με αυτήν την πολιτική.
- 12.2.3 Σε περίπτωση που το είδος της επεξεργασίας, ιδίως με τη χρήση των νέων τεχνολογιών και λαμβάνοντας υπόψη τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας, είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο Όμιλος πρέπει, πριν από τη διεξαγωγή της επεξεργασίας, να προβεί σε αξιολόγηση των επιπτώσεων των προβλεπόμενων πράξεων επεξεργασίας στην προστασία των προσωπικών δεδομένων. Μια ενιαία ΕΕΠΔ μπορεί να εκτιμήσει μια σειρά παρόμοιων διαδικασιών επεξεργασίας που παρουσιάζουν παρόμοιους υψηλούς κινδύνους.
- 12.2.4 Όταν, ως αποτέλεσμα της ΕΕΠΔ, είναι σαφές ότι ο Όμιλος πρόκειται να αρχίσει την επεξεργασία δεδομένων προσωπικού χαρακτήρα που θα μπορούσαν να προκαλέσουν ζημία στα υποκείμενα των δεδομένων, η απόφαση για το αν θα πρέπει να προχωρήσει ο Όμιλος στην επεξεργασία πρέπει να αποσταλεί για έλεγχο προς τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ/DPO).
- 12.2.5 Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO) πρέπει, εφόσον υπάρχουν σημαντικές αμφιβολίες, είτε ως προς την πιθανή βλάβη των υποκειμένων των δεδομένων, είτε λόγω του μεγάλου όγκου των δεδομένων προσωπικού χαρακτήρα, να απευθύνει το θέμα στην εποπτική αρχή.
- 12.2.6 Επιλέγονται οι κατάλληλοι μηχανισμοί ελέγχου και τίθενται σε εφαρμογή για να μειωθεί το επίπεδο κινδύνου όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε αποδεκτό επίπεδο, με αναφορά στα τεκμηριωμένα κριτήρια αποδοχής κινδύνου που έχει θεσπίσει ο Όμιλος και τις απαιτήσεις του Κανονισμού GDPR.

### 13. ΙΔΙΟΚΤΗΣΙΑ ΕΓΓΡΑΦΟΥ ΚΑΙ ΈΓΚΡΙΣΗ

Ο Όμιλος είναι ο κάτοχος αυτού του εγγράφου και είναι υπεύθυνος για την αναθεώρηση αυτής της Πολιτικής.

Μια τρέχουσα έκδοση αυτού του εγγράφου είναι διαθέσιμη σε όλα τα μέλη του προσωπικού στο εταιρικό Portal και δημοσιεύεται στην ηλεκτρονική διεύθυνση:

<https://superfast.sharepoint.com/Pages/Home.aspx>.

Η πολιτική αυτή εγκρίθηκε την Τετάρτη 21/04/2021.