1. Σκοπός

Η παρούσα Πολιτική καθορίζει το πλαίσιο συμμόρφωσης του Ομίλου ΝΕΡΑ ΚΡΗΤΗΣ ΑΒΕΕ με τον Κανονισμό (ΕΕ) 2016/679 (GDPR) και την ισχύουσα εθνική νομοθεσία περί προστασίας προσωπικών δεδομένων. Στόχος είναι:

- Η νόμιμη, διαφανής και ασφαλής επεξεργασία προσωπικών δεδομένων
- Η προστασία των δικαιωμάτων πελατών, εργαζομένων και συνεργατών
- Η αποτροπή παραβιάσεων και διοικητικών κυρώσεων

---

2. Πεδίο Εφαρμογής

Η Πολιτική εφαρμόζεται:

- Σε όλα τα τμήματα του Ομίλου
- Σε όλους τους εργαζόμενους
- Σε εξωτερικούς συνεργάτες που επεξεργάζονται δεδομένα για λογαριασμό της εταιρείας

---

3. Ορισμοί

Προσωπικά Δεδομένα: Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.
Επεξεργασία: Κάθε πράξη που πραγματοποιείται σε προσωπικά δεδομένα (συλλογή, αποθήκευση, διαβίβαση κ.λπ.).
Υπεύθυνος Επεξεργασίας: Η ΝΕΡΑ ΚΡΗΤΗΣ ΑΒΕΕ για τα δεδομένα που διαχειρίζεται.

---

4. Αξιολόγηση Συμμόρφωσης με τον GDPR

Ο Όμιλος εφαρμόζει συστηματική διαδικασία αξιολόγησης συμμόρφωσης που περιλαμβάνει:

4.1 Χαρτογράφηση Δεδομένων

- Καταγραφή κατηγοριών προσωπικών δεδομένων (πελατών, εργαζομένων, προμηθευτών)
- Προσδιορισμός σκοπού και νομικής βάσης επεξεργασίας

- Καθορισμός χρόνου διατήρησης

4.2 Μητρώο Δραστηριοτήτων Επεξεργασίας

Τηρείται επικαιροποιημένο αρχείο σύμφωνα με το άρθρο 30 του GDPR.

4.3 Αξιολόγηση Κινδύνων

Διενεργείται περιοδική εκτίμηση κινδύνου για:

- Μη εξουσιοδοτημένη πρόσβαση
- Απώλεια ή αλλοίωση δεδομένων
- Κυβερνοεπιθέσεις

Όπου απαιτείται, πραγματοποιείται DPIA (Data Protection Impact Assessment).

4.4 Τεχνικά & Οργανωτικά Μέτρα

Εφαρμόζονται μέτρα όπως:

- Έλεγχος πρόσβασης με κωδικούς
- Περιορισμός δικαιωμάτων χρηστών
- Antivirus & firewall
- Κρυπτογράφηση όπου απαιτείται
- Φυσική ασφάλεια αρχείων

4.4.1 Υποδομή Μηχανογράφησης & Δικτυακή Ασφάλεια

Για την προστασία των προσωπικών δεδομένων που τηρούνται/διακινούνται στα πληροφοριακά συστήματα, εφαρμόζονται επιπλέον τα ακόλουθα τεχνικά μέτρα και πρακτικές λειτουργίας:

• Servers & Virtualization: Σκλήρυνση (hardening) λειτουργικών, τακτικές ενημερώσεις (patching), περιορισμός υπηρεσιών/θυρών, διακριτοί λογαριασμοί διαχειριστών και αρχή ελάχιστου δικαιώματος (least privilege).

• Storage: Έλεγχος πρόσβασης σε επίπεδο συστήματος/φακέλων, παρακολούθηση χωρητικότητας και υγείας, χρήση snapshots όπου υποστηρίζεται και περιοδικός έλεγχος ακεραιότητας.

• Backup: Εφαρμογή κανόνα 3-2-1 (πολλαπλά αντίγραφα, διαφορετικά μέσα, ένα αντίγραφο εκτός εγκατάστασης ή/και αμετάβλητο - immutable). Καθορισμένα retention, περιοδικές δοκιμές επαναφοράς (restore tests) και διακριτά διαπιστευτήρια/πρόσβαση για την υποδομή backup.

• Switches/Firewalls: Διακριτό Management VLAN για διαχείριση, απενεργοποίηση μη ασφαλών πρωτοκόλλων διαχείρισης, ενημέρωση firmware, καταγραφή αλλαγών

ρυθμίσεων και εφαρμογή πολιτικής "default deny" με ρητούς κανόνες μεταξύ ζωνών/VLANs.

• Ασύρματο δίκτυο (WiFi): Τρία διακριτά SSIDs με πλήρως διαχωρισμένα VLANs (Staff, Guest, Corporate). Το Guest και το Staff παρέχει πρόσβαση μόνο στο διαδίκτυο, ενώ το Corporate παρέχει πρόσβαση στις αναγκαίες εταιρικές υπηρεσίες. Εφαρμόζεται WPA2 και ισχυρή πολιτική κωδικών με περιοδική αλλαγή.

• PCs/Laptops εργαζομένων: Κεντρική διαχείριση ενημερώσεων, προστασία endpoint (AV/EDR), πολιτικές ισχυρών κωδικών/MFA όπου υποστηρίζεται και περιορισμός τοπικών διαχειριστικών δικαιωμάτων.

• File Server: Δικαιώματα πρόσβασης μέσω ομάδων (RBAC), αρχή "need-to-know", καταγραφή πρόσβασης/αλλαγών σε κρίσιμους φακέλους (auditing) και περιοδική ανασκόπηση δικαιωμάτων.

• Καταγραφή & Παρακολούθηση: Κεντρική συλλογή συμβάντων (logs) από servers, firewall και κρίσιμες συσκευές δικτύου, καθώς και ειδοποιήσεις για σημαντικά γεγονότα (αποτυχημένες συνδέσεις, αλλαγές πολιτικών, αποτυχίες backup, ανωμαλίες).

4.5 Διαχείριση Παραβίασης Δεδομένων

Υπάρχει διαδικασία:

- Άμεσης εσωτερικής αναφοράς περιστατικού
- Αξιολόγησης σοβαρότητας
- Ενημέρωσης Αρχής Προστασίας Δεδομένων εντός 72 ωρών (όπου απαιτείται)
- Ενημέρωσης υποκειμένων δεδομένων εφόσον απαιτείται

4.6 Περιοδικός Έλεγχος Συμμόρφωσης

Η συμμόρφωση επανεξετάζεται:

- Ετησίως
- Σε περίπτωση αλλαγής δραστηριοτήτων
- Μετά από περιστατικό παραβίασης

---

5. Νομιμότητα Επεξεργασίας

Η επεξεργασία πραγματοποιείται μόνο όταν υπάρχει νόμιμη βάση όπως:

- Εκτέλεση σύμβασης
- Νομική υποχρέωση
- Έννομο συμφέρον

- Συγκατάθεση

---

6. Δικαιώματα Υποκειμένων

Η εταιρεία διασφαλίζει:

- Δικαίωμα πρόσβασης
- Δικαίωμα διόρθωσης
- Δικαίωμα διαγραφής
- Δικαίωμα περιορισμού επεξεργασίας
- Δικαίωμα φορητότητας
- Δικαίωμα εναντίωσης

Αιτήματα εξετάζονται εντός ενός (1) μηνός.

---

7. Υποχρέωση Εμπιστευτικότητας Εργαζομένων

7.1 Υπογραφή Δήλωσης Εμπιστευτικότητας

Όλοι οι εργαζόμενοι που έρχονται σε επαφή με προσωπικά δεδομένα:

- Υπογράφουν ρήτρα εμπιστευτικότητας κατά την πρόσληψη
- Δεσμεύονται γραπτώς για τήρηση απορρήτου
- Υποχρεούνται να χρησιμοποιούν τα δεδομένα μόνο για υπηρεσιακούς σκοπούς

Η υποχρέωση εμπιστευτικότητας συνεχίζει να ισχύει και μετά τη λήξη της εργασιακής σχέσης.

7.2 Περιορισμός Πρόσβασης

Η πρόσβαση σε προσωπικά δεδομένα παρέχεται:

- Μόνο σε εξουσιοδοτημένο προσωπικό
- Με βάση την αρχή “need-to-know”

---

8. Εκπαίδευση Προσωπικού

Ο Όμιλος:

- Παρέχει περιοδική εκπαίδευση GDPR
- Ενημερώνει για κινδύνους phishing και κυβερνοασφάλειας
- Τεκμηριώνει τη συμμετοχή σε εκπαιδεύσεις

---

9. Διαβίβαση σε Τρίτους

Οποιαδήποτε διαβίβαση δεδομένων σε:

- Λογιστές
- Νομικούς
- IT παρόχους

Πραγματοποιείται μόνο κατόπιν σύμβασης επεξεργασίας δεδομένων (Data Processing Agreement).

---

10. Κυρώσεις

Η παραβίαση της παρούσας Πολιτικής μπορεί να επιφέρει:

- Πειθαρχικές κυρώσεις
- Απόλυση
- Αστικές ή ποινικές ευθύνες

---

11. Αναθεώρηση Πολιτικής

Η παρούσα Πολιτική:

- Αναθεωρείται ετησίως
- Επικαιροποιείται σε περίπτωση νομοθετικών αλλαγών

ΝΕΡΑ ΚΡΗΤΗΣ ΑΒΕΕ
ΒΙΟΜΗΧΑΝΙΑ ΠΛΑΣΤΙΚΩΝ - ΕΜΦΙΑΔΩΣΗ ΝΕΡΟΥ
ΑΡΙΣΤΕΙΔΟΥ 1 - ΒΥΛΙΚΑΡΝΑΙ
ΑΦΜ: 099360920 ΔΟΥ: ΦΑΕ ΑΘΗΝΩΝ
ΑΡΙΘΜΟΣ ΓΕΜΗ: 121501000

Ο Διευθύνων Σύμβουλος

Ημ/νια Αναθεώρησης: 30/1/2026