



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΕΡΙΦΕΡΕΙΑΚΟΣ ΣΥΝΔΕΣΜΟΣ
ΦΟΡΕΩΝ ΔΙΑΧΕΙΡΙΣΗΣ
ΣΤΕΡΕΩΝ ΑΠΟΒΛΗΤΩΝ
(Φο.Δ.Σ.Α.)
ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

Αρ. Συνεδρίασης : 1^η/09.03.2026
Αριθμός Απόφασης: 4

ΑΠΟΣΠΑΣΜΑ
ΑΠΟ ΤΟ 1^ο ΠΡΑΚΤΙΚΟ ΤΗΣ ΣΥΝΕΔΡΙΑΣΗΣ ΤΟΥ ΔΙΟΙΚΗΤΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ ΤΟΥ ΠΕΡΙΦΕΡΕΙΑΚΟΥ
ΣΥΝΔΕΣΜΟΥ ΦΟΔΣΑ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΘΕΜΑ 3^ο ΗΜΕΡΗΣΙΑΣ ΔΙΑΤΑΞΗΣ: Επικαιροποίηση Πολιτικής Ασφάλειας.

Σήμερα την 9^η του μηνός **Μαρτίου**, έτους **2026**, ημέρα **Δευτέρα** και ώρα **12:00** πραγματοποιήθηκε η **1^η Συνεδρίαση** του Διοικητικού Συμβουλίου του Περιφερειακού Συνδέσμου ΦΟΔΣΑ Κεντρικής Μακεδονίας, **δια ζώσης και ταυτόχρονα με τηλεδιάσκεψη** (μεικτή συνεδρίαση), στην αίθουσα συνεδριάσεων του Δημοτικού Συμβουλίου του Δήμου Θεσσαλονίκης (Δημαρχείο Θεσσαλονίκης, Βασ. Γεωργίου Α΄ 1), κατόπιν της υπ' αριθμ. **2734/05-03-2026** έγγραφης **πρόσκλησης** του Προέδρου, κ. Μιχαήλ Γεράνη, που επιδόθηκε νομίμως και εμπροθέσμως στον καθένα από τους αντιπροσώπους, σύμφωνα με το άρθρο 67 του Ν. 3852/2010 όπως τροποποιήθηκε και ισχύει και το άρθρο 6 του Ν. 5056/2023, καθώς και τις υπ' αρ.98/Α.Π. 8182/26-01-2024 (ΑΔΑ: 9ΝΚ84ΜΤΛ6-Π6Λ) και υπ' αρ. 36133/17.04.2024 (ΑΔΑ: 9ΑΘΒ46ΜΤΛ6-Χ8Π) εγκυκλίου του Υπουργείου Εσωτερικών.

Διαπιστώθηκε ότι σε σύνολο **εξήντα οκτώ (68)** εκπροσώπων, παρόντες ήταν οι παρακάτω:

ΠΑΡΟΝΤΕΣ

1.	ΑΛΕΞΑΝΔΡΕΙΑΣ	ΠΑΓΓΟΥΡΑΣ ΑΘΑΝΑΣΙΟΣ	
2.	ΑΛΕΞΑΝΔΡΕΙΑΣ	ΤΟΚΑΣ ΣΩΤΗΡΙΟΣ	Τηλεδιάσκεψη
3.	ΑΜΠΕΛΟΚΗΠΩΝ - ΜΕΝΕΜΕΝΗΣ	ΚΥΡΙΖΟΓΛΟΥ ΛΑΖΑΡΟΣ	
4.	ΑΜΠΕΛΟΚΗΠΩΝ - ΜΕΝΕΜΕΝΗΣ	ΚΟΥΣΙΔΗΣ ΓΕΩΡΓΙΟΣ	
5.	ΑΡΙΣΤΟΤΕΛΗ	ΒΑΛΙΑΝΟΣ ΣΤΥΛΙΑΝΟΣ	Τηλεδιάσκεψη

6.	ΒΕΡΟΙΑΣ	ΠΑΠΑΔΟΠΟΥΛΟΣ ΒΑΣΙΛΕΙΟΣ	
7.	ΒΕΡΟΙΑΣ	ΤΣΙΛΟΓΙΑΝΝΗΣ ΓΕΩΡΓΙΟΣ	Τηλεδιάσκεψη
8.	ΒΙΣΑΛΤΙΑΣ	ΚΟΤΣΑΝΠΑΠΑΣ ΧΑΡΙΣΣΗΣ	Τηλεδιάσκεψη
9.	ΒΟΛΒΗΣ	ΛΙΑΜΑΣ ΔΙΑΜΑΝΤΗΣ	Τηλεδιάσκεψη
10.	ΔΙΟΥ-ΟΛΥΜΠΟΥ	ΣΠΑΘΑΡΗΣ ΝΙΚΟΛΑΟΣ	Τηλεδιάσκεψη
11.	ΕΜΜΑΝΟΥΗΛ ΠΑΠΠΑ	ΝΟΤΑΣ ΔΗΜΗΤΡΙΟΣ	
12.	ΗΡΑΚΛΕΙΑΣ	ΤΕΒΕΚΕΛΗΣ ΒΑΣΙΛΕΙΟΣ	
13.	ΘΕΡΜΑΪΚΟΥ	ΤΖΕΚΟΣ ΘΕΟΔΩΡΟΣ	Τηλεδιάσκεψη
14.	ΘΕΡΜΑΪΚΟΥ	ΧΑΤΖΗΠΑΝΑΓΙΩΤΗΣ ΠΑΝΑΓΙΩΤΗΣ	Τηλεδιάσκεψη
15.	ΘΕΡΜΗΣ	ΠΑΠΑΔΟΠΟΥΛΟΣ ΘΕΟΔΩΡΟΣ	Τηλεδιάσκεψη
16.	ΘΕΡΜΗΣ	ΓΚΙΖΑΡΗΣ ΣΤΕΡΓΙΟΣ	Τηλεδιάσκεψη
17.	ΘΕΣΣΑΛΟΝΙΚΗΣ	ΑΓΓΕΛΟΥΔΗΣ ΣΤΥΛΙΑΝΟΣ	
18.	ΘΕΣΣΑΛΟΝΙΚΗΣ	ΔΗΜΑΡΕΛΟΣ ΓΕΩΡΓΙΟΣ	
19.	ΘΕΣΣΑΛΟΝΙΚΗΣ	ΖΑΧΑΡΙΑΔΗΣ ΛΑΖΑΡΟΣ	
20.	ΘΕΣΣΑΛΟΝΙΚΗΣ	ΚΥΡΙΖΙΔΗΣ ΕΦΡΑΙΜ	
21.	ΚΑΛΑΜΑΡΙΑΣ	ΑΡΑΠΟΓΛΟΥ ΧΡΥΣΗ	Τηλεδιάσκεψη
22.	ΚΑΛΑΜΑΡΙΑΣ	ΤΣΙΡΑΜΠΙΔΟΥ ΜΑΙΡΗ	
23.	ΚΑΛΑΜΑΡΙΑΣ	ΤΕΜΕΚΕΝΙΔΗΣ ΑΡΙΣΤΟΤΕΛΗΣ	
24.	ΚΑΣΣΑΝΔΡΑΣ	ΛΕΙΒΑΔΙΩΤΗΣ ΗΡΑΚΛΗΣ	Τηλεδιάσκεψη
25.	ΚΑΤΕΡΙΝΗΣ	ΤΑΠΡΑΣ ΗΛΙΑΣ	
26.	ΚΑΤΕΡΙΝΗΣ	ΚΥΡΙΑΚΙΔΗΣ ΓΕΩΡΓΙΟΣ	
27.	ΚΙΛΚΙΣ	ΣΗΜΑΙΟΦΟΡΙΔΗΣ ΑΛΕΞΑΝΔΡΟΣ	Τηλεδιάσκεψη
28.	ΚΙΛΚΙΣ	ΠΑΠΑΚΩΣΤΑΣ ΚΩΝΣΤΑΝΤΙΝΟΣ	Τηλεδιάσκεψη

29.	ΛΑΓΚΑΔΑ	ΑΝΔΡΕΑΔΟΥ ΕΛΠΙΝΙΚΗ	Τηλεδιάσκεψη
30.	ΝΑΟΥΣΑΣ	ΚΟΥΤΣΟΓΙΑΝΝΗΣ ΝΙΚΟΛΑΟΣ	Τηλεδιάσκεψη
31.	ΝΑΟΥΣΑΣ	ΣΑΜΑΡΑΣ ΓΡΗΓΟΡΙΟΣ	
32.	ΝΕΑΠΟΛΗΣ- ΣΥΚΕΩΝ	ΖΑΡΙΦΗΣ ΙΩΑΝΝΗΣ	
33.	ΝΕΑΣ ΖΙΧΝΗΣ	ΜΠΟΖΗΣ ΠΑΝΤΕΛΗΣ	Τηλεδιάσκεψη
34.	ΠΕΛΛΑΣ	ΦΟΥΝΤΟΥΚΙΔΗΣ ΕΥΣΤΑΘΙΟΣ	
35.	ΠΥΛΑΙΑΣ- ΧΟΡΤΙΑΤΗ	ΚΑΪΤΕΖΙΔΗΣ ΙΓΝΑΤΙΟΣ	
36.	ΠΥΛΑΙΑΣ -ΧΟΡΤΙΑΤΗ	ΓΕΡΑΝΗΣ ΜΙΧΑΛΗΣ	
37.	ΣΚΥΔΡΑΣ	ΙΓΝΑΤΙΑΔΟΥ ΑΙΚΑΤΕΡΙΝΗ	Τηλεδιάσκεψη
38.	ΧΑΛΚΗΔΟΝΟΣ	ΑΝΑΓΝΩΣΤΟΠΟΥΛΟΣ ΣΤΑΥΡΟΣ	Τηλεδιάσκεψη
39.	ΩΡΑΙΟΚΑΣΤΡΟΥ	ΤΣΑΚΙΡΗΣ ΠΑΝΤΕΛΕΗΜΩΝ	Τηλεδιάσκεψη
40.	Το ορισμένο από τους εργαζόμενους μέλος	ΙΩΑΝΝΙΔΗΣ ΒΑΣΙΛΕΙΟΣ	

Σύνολο: Σαράντα (40) Μέλη

ΑΠΟΝΤΕΣ

1.	ΑΛΜΠΩΠΙΑΣ	ΠΑΡΟΥΤΟΓΛΟΥ ΝΙΚΟΛΑΟΣ
2.	ΑΜΦΙΠΟΛΗΣ	ΠΑΠΑΔΟΠΟΥΛΟΣ ΙΟΑΡΔΑΝΗΣ
3.	ΔΕΛΤΑ	ΚΙΟΥΤΣΟΥΚΗΣ ΦΩΤΙΟΣ
4.	ΔΕΛΤΑ	ΧΑΛΚΙΔΗΣ ΔΗΜΗΤΡΙΟΣ
5.	ΕΔΕΣΣΑΣ	ΤΣΕΠΚΕΝΤΖΗΣ ΙΩΑΝΝΗΣ
6.	ΘΕΣΣΑΛΟΝΙΚΗΣ	ΚΙΡΛΑΣ ΔΗΜΗΤΡΙΟΣ
7.	ΚΑΤΕΡΙΝΗΣ	ΟΦΕΙΔΗΣ ΣΑΒΒΑΣ
8.	ΚΟΡΔΕΛΙΟΥ-ΕΥΟΣΜΟΥ	ΑΛΕΞΑΝΔΡΙΔΗΣ ΕΛΕΥΘΕΡΙΟΣ

9.	ΚΟΡΔΕΛΙΟΥ-ΕΥΟΣΜΟΥ	ΜΑΞΟΥΡΑΣ ΓΕΩΡΓΙΟΣ
10.	ΚΟΡΔΕΛΙΟΥ-ΕΥΟΣΜΟΥ	ΔΕΜΕΡΤΖΗΣ ΧΡΗΣΤΟΣ
11.	ΛΑΓΚΑΔΑ	ΡΟΦΑΛΙΚΟΣ ΓΕΩΡΓΙΟΣ
12.	ΝΕΑΠΟΛΗΣ ΣΥΚΕΩΝ	ΔΑΝΙΗΛΙΔΗΣ ΣΥΜΕΩΝ
13.	ΝΕΑΠΟΛΗΣ ΣΥΚΕΩΝ	ΤΡΙΛΥΡΑΚΗΣ ΣΤΑΥΡΟΣ
14.	ΝΕΑΣ ΠΡΟΠΟΝΤΙΔΑΣ	ΚΑΡΡΑΣ ΕΜΜΑΝΟΥΗΛ
15.	ΝΕΑΣ ΠΡΟΠΟΝΤΙΔΑΣ	ΘΕΡΓΙΟΣ ΝΙΚΟΛΑΟΣ
16.	ΠΑΙΟΝΙΑΣ	ΓΚΑΪΤΑΤΖΗΣ ΣΤΥΛΙΑΝΟΣ
17.	ΠΑΥΛΟΥ ΜΕΛΑ	ΚΟΡΑΪΔΗΣ ΚΟΣΜΑΣ
18.	ΠΑΥΛΟΥ ΜΕΛΑ	ΣΙΒΗΣ ΝΙΚΟΛΑΟΣ
19.	ΠΑΥΛΟΥ ΜΕΛΑ	ΛΑΖΑΡΙΔΗΣ ΑΘΑΝΑΣΙΟΣ
20.	ΠΕΛΛΑΣ	ΔΟΝΤΣΗΣ ΝΙΚΟΛΑΟΣ
21.	ΠΟΛΥΓΥΡΟΥ	ΕΜΜΑΝΟΥΗΛ ΓΕΩΡΓΙΟΣ
22.	ΠΥΔΝΑΣ-ΚΟΛΙΝΔΡΟΥ	ΚΟΜΠΑΤΣΙΑΡΗΣ ΧΡΗΣΤΟΣ
23.	ΣΕΡΡΩΝ	ΜΗΤΛΙΑΓΚΑ ΒΑΡΒΑΡΑ
24.	ΣΕΡΡΩΝ	ΜΙΧΤΣΟΓΛΟΥ ΔΗΜΗΤΡΙΟΣ
25.	ΣΙΘΩΝΙΑΣ	ΜΑΛΛΙΝΗΣ ΙΩΑΝΝΗΣ
26.	ΣΙΝΤΙΚΗΣ	ΤΑΤΣΙΟΣ ΓΕΩΡΓΙΟΣ
27.	ΧΑΛΚΗΔΟΝΟΣ	ΚΟΡΔΟΝΟΥΡΗΣ ΜΕΝΕΛΑΟΣ
28.	ΩΡΑΙΟΚΑΣΤΡΟΥ	ΔΗΜΗΤΡΙΑΔΟΥ ΣΟΦΙΑ

Σύνολο: Είκοσι οκτώ (28) Μέλη

Πριν τη συζήτηση των θεμάτων της ημερήσιας διάταξης, το Διοικητικό Συμβούλιο αποφάσισε ομόφωνα για το κατεπείγον ενός (1) έκτακτου θέματος, σύμφωνα με του αρ. 67, παρ. 7 του ν. 3852/2010, όπως τροποποιήθηκε και ισχύει.

Τα πρακτικά της Συνεδρίασης τηρήθηκαν από τη γραμματέα του Διοικητικού Συμβουλίου κα Κυριακή Ιωαννίδου, υπάλληλο του Περιφερειακού Συνδέσμου Φο.Δ.Σ.Α. Κεντρικής Μακεδονίας (ΠΕ Διοικητικού-Οικονομικού).

Ο Πρόεδρος του Περιφερειακού Συνδέσμου Φορέων Διαχείρισης Στερεών Αποβλήτων (Φο.Δ.Σ.Α.) Κεντρικής Μακεδονίας, κ. Μιχαήλ Γεράνης, ύστερα από τη διαπίστωση της νόμιμης σύγκλισης και νόμιμης απαρτίας, κήρυξε την έναρξη της συνεδρίασης, γιατί σε σύνολο **εξήντα οκτώ (68)** αντιπροσώπων βρέθηκαν παρόντες **σαράντα (40) αντιπρόσωποι**.

Κατόπιν, εισηγούμενος το 3^ο θέμα της ημερήσιας διάταξης σχετικά με την «Επικαιροποίηση Πολιτικής Ασφάλειας», έθεσε υπόψη των μελών του Δ.Σ.:

1. Την υπ'αρ. 17364/12.12.2025 εισήγηση του Αναπληρωτή Προϊσταμένου του Τμήματος Πληροφορικής, Τηλεπικοινωνιών και Ασφάλειας Συστημάτων:
2. Την υπ'αρ. 395/2025 (ΑΔΑ: 9ΨΔ0ΟΞΧΝ-9ΞΞ) εισήγηση-απόφαση της Εκτελεστικής Επιτροπής με θέμα «Επικαιροποίηση Πολιτικής Ασφάλειας», στην οποία αναφέρονται τα εξής:

«Η Πολιτική Ασφάλειας είναι μια δημοσιοποίηση ενός συνόλου κανόνων που αφορούν τις μεθόδους διαχείρισης των προσωπικών δεδομένων εκ μέρους του φορέα. Αυτές οι μέθοδοι αφορούν τη διαφύλαξη, την προστασία και την προσβασιμότητα του φυσικού και ηλεκτρονικού αρχείου που τηρεί ο φορέας.

Η εκπόνηση αλλά και η εφαρμογή της Πολιτικής Ασφάλειας του φορέα βασίζεται:

A) Στο άρθρο 24 από τον Γενικό Κανονισμό Προστασίας Δεδομένων 679/2016:

«Ευθύνη του υπευθύνου επεξεργασίας

1. *Λαμβάνοντας υπόψη 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, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο.»*

B) στο άρθρο 22 Ν.4624/2019 (ΦΕΚ 137Α/29-08-2019)

«Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα

3. Στις περιπτώσεις των προηγούμενων παραγράφων λαμβάνονται όλα τα κατάλληλα και ειδικά μέτρα για τη διαφύλαξη των συμφερόντων του υποκειμένου των δεδομένων προσωπικού χαρακτήρα. Λαμβάνοντας υπόψη την κατάσταση της τεχνολογίας, το κόστος εφαρμογής και τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους που θέτει, ανάλογα με τη σοβαρότητά τους στα δικαιώματα και στις ελευθερίες των φυσικών προσώπων η επεξεργασία αυτή, στα μέτρα αυτά μπορούν να περιλαμβάνονται ιδίως:

α) τεχνικά και οργανωτικά μέτρα που διασφαλίζουν ότι η επεξεργασία είναι σύμφωνη με τον ΓΚΠΔ.

β) μέτρα για να διασφαλιστεί ότι είναι δυνατή η εκ των υστέρων επαλήθευση και ο προσδιορισμός του εάν και από ποιον έχουν εισαχθεί, τροποποιηθεί ή αφαιρεθεί τα προσωπικά δεδομένα.

γ) μέτρα για την ενδυνάμωση της ευαισθητοποίησης του προσωπικού που ασχολείται με την επεξεργασία.

δ) περιορισμοί πρόσβασης από τους υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία.

ε) η ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα

στ) η κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα

ζ) μέτρα για τη διασφάλιση της ικανότητας, της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της ανθεκτικότητας των συστημάτων και υπηρεσιών επεξεργασίας που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της δυνατότητας ταχείας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε περίπτωση φυσικού ή τεχνικού συμβάντος.»

Γ) Στο άρθρο 8.2 ΦΕΚ 3805Β/2021 και στο άρθρο 15 Β.1 ΦΕΚ 3805Β/2023 Οργανισμός Εσωτερικής Υπηρεσίας

«Αρμοδιότητες Διεύθυνσης Αναπτυξιακού Προγραμματισμού Παρακολούθησης και Πληροφορικής, Β.1.3 Τμήμα Πληροφορικής Τηλεπικοινωνιών & Ασφάλειας Συστημάτων»

Σχεδιάζει την πολιτική ασφάλειας των συστημάτων και μεριμνά για την ακεραιότητα των πληροφοριακών δεδομένων».

Στο πλαίσιο αυτό, ο Περιφερειακός Σύνδεσμος Φορέων Διαχείρισης Στερεών Αποβλήτων (Φο.Δ.Σ.Α.) Κεντρικής Μακεδονίας προχώρησε στην σύσταση ομάδας εργασίας με την Απόφαση

Προέδρου 202/2018 (Αρ. πρωτ. 16325/29-10-2018) και εκπόνησε την πολιτικής ασφάλειας η οποία περιλαμβάνει κυρίως:

- Το εισαγωγικό κείμενο για τον αναγνώστη,
- Τον σκοπό της πολιτικής ασφάλειας του φορέα,
- Επεξήγηση του όρου δεδομένα προσωπικού χαρακτήρα,
- Τρόπους και τα είδη συλλογής δεδομένων προσωπικού για υπαλλήλους και αναδόχους και της νομικής βάσης που διέπεται,
- Χρόνους τήρησης των δεδομένων προσωπικού χαρακτήρα,
- Τα δικαιώματα των υποκειμένων,
- Τη διαβίβαση δεδομένων σε τρίτους,
- Τα μέτρα ασφάλειας του φορέα,
- Τη σύναψη συμφωνητικών εμπιστευτικότητας,
- Τα στοιχεία του Υπευθύνου Προστασίας Δεδομένων του φορέα και της Αρχής Προστασίας Δεδομένων,
- Στοιχεία επικοινωνίας των υποκειμένων με τον φορέα.
- Πολιτική Ασφάλειας Επεξεργασίας Αρχείων

Εγκρίθηκε με την Αρ. Απόφασης 8/2022 (ΑΔΑ:ΨΧΕΨΟΞΧΝ-ΗΧΗ) του ΔΣ του φορέα στις 10/11/2022. Ωστόσο στο διάστημα αυτό, άλλαξαν τα είδη προσωπικών δεδομένων που επεξεργάζεται ο φορέας, η πολιτική διαγραφής αρχείων αλλά και η πολιτική ασφάλειας που ενσωματώνεται στην πολιτική προστασίας. Η πολιτική ασφαλείας εμπλουτίστηκε με νέους κανόνες, οι οποίοι δεν είναι πλέον συμβουλευτικοί αλλά δεσμευτικοί.

Κατόπιν των ανωτέρω, εισηγούμαστε την έγκριση της επικαιροποιημένης συνημμένης Πολιτικής Ασφάλειας και λόγω της ουσιώδους σημασίας του θέματος προτείνουμε την έγκρισή του από το Διοικητικό Συμβούλιο του φορέα».

Ως εκ τούτου, το Διοικητικό Συμβούλιο, μετά από διαλογική συζήτηση, προχώρησε σε ψηφοφορία, έχοντας λάβει υπόψη της όλα τα ανωτέρω, όπως επίσης και:

- Το άρθρο 95 του Ν. 3463/2006,
- Τα άρθρα 65 και 67 του Ν. 3852/2010, όπως τροποποιήθηκε και ισχύει,
- Τα άρθρα 231 και 232 του ν. 4555/2018 (ΦΕΚ 133/Α'/19-07-2018):

Ψήφισαν:**Υπέρ:** Σαράντα (40) Μέλη

Κατόπιν των ανωτέρω, το Διοικητικό Συμβούλιο ενέκρινε το θέμα και προχώρησε στη λήψη της παρακάτω απόφασης:

ΑΠΟΦΑΣΙΖΕΙ ΟΜΟΦΩΝΑ

Εγκρίνει την Επικαιροποίηση της Πολιτικής Ασφάλειας του Περιφερειακού Συνδέσμου Φο.Δ.Σ.Α. Κεντρικής Μακεδονίας, η οποία αποτελεί αναπόσπαστο τμήμα της παρούσας απόφασης.

Η απόφαση αυτή έλαβε αύξοντα αριθμό 4/2026.

Για το παραπάνω θέμα συντάχθηκε το παρόν πρακτικό και υπογράφεται ως εξής:

Η ΓΡΑΜΜΑΤΕΑΣ**Ο ΠΡΟΕΔΡΟΣ ΤΟΥ Δ.Σ.**

ΚΥΡΙΑΚΗ ΙΩΑΝΝΙΔΟΥ
ΠΕ Διοικητικού-Οικονομικού

ΜΙΧΑΗΛ ΓΕΡΑΝΗΣ
Πρόεδρος Δ.Σ.
Δήμου Πυλαίας-Χορτιάτη



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΕΡΙΦΕΡΕΙΑΚΟΣ ΣΥΝΔΕΣΜΟΣ
ΦΟΡΕΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΣΤΕΡΕΩΝ
ΑΠΟΒΛΗΤΩΝ (Φο.Δ.Σ.Α)
ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΑΡΧΕΙΩΝ

ΔΕΚΕΜΒΡΙΟΣ 2025

Περιεχόμενα

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΑΡΧΕΙΩΝ	1
<i>Προοίμιο</i>	<i>5</i>
<i>Εισαγωγή</i>	<i>6</i>
1) Γλωσσάριο - Συντομογραφίες.....	6
2) Σκοπός.....	7
3) Βασικές έννοιες και ορισμοί Γ.Κ.Π.Δ.....	7
4) Αρχές Νόμιμης Επεξεργασίας (Άρθρα 5 & 6 ΓΚΠΔ)	7
5) Ρόλος και Αρμοδιότητες του Τμήματος Πληροφορικής	8
6) Κυρώσεις σε Περίπτωση Μη Συμμόρφωσης	8
Πολιτική Προστασίας Προσωπικών Δεδομένων	10
<i>Εισαγωγή</i>	<i>10</i>
1) Σκοπός.....	10
2) Τί είναι τα δεδομένα προσωπικού χαρακτήρα	11
3) Συλλογή.....	11
3α) Τρόποι Συλλογής Δεδομένων	11
3β) Ποια δεδομένα συλλέγονται:	12
i. Στοιχεία Ταυτοποίησης και Επικοινωνίας	12
ii. Διοικητικά, Μισθολογικά και Ασφαλιστικά Στοιχεία	12
iii. Στοιχεία Επαγγελματικής Κατάστασης και Προσόντων	12
iv. Ποινικά και Δικαστικά Δεδομένα (όπου απαιτείται από τη νομοθεσία)	12
v. Δεδομένα Υγείας (Ειδικές Κατηγορίες Δεδομένων – Άρθρο 9 Γ.Κ.Π.Δ.).....	13
vi. Δεδομένα που περιλαμβάνονται σε υποβληθέντα δικαιολογητικά και έγγραφα.....	13
vi. Δεδομένα που περιλαμβάνονται σε ψηφιακές βάσεις δεδομένων του ελληνικού δημοσίου.....	13
I. Στοιχεία Ταυτοποίησης Προσώπων που συμμετέχουν στη διαδικασία	14
II. Φορολογικά, Ασφαλιστικά και Οικονομικά Δεδομένα	14
III. Νομικά Έγγραφα και Πιστοποιήσεις Επιχειρηματικής Ικανότητας	14
IV. Στοιχεία Τεχνικής & Επαγγελματικής Ικανότητας	14
V. Ποινικά Δεδομένα (όπου το απαιτεί η νομοθεσία δημοσίων συμβάσεων)	15
<i>Παροχή πρόσθετων δεδομένων εκ μέρους προσφερόντων</i>	<i>15</i>
3γ) Για ποιους λόγους συλλέγονται/Νομική βάση	15
4) Χρόνος τήρησης των δεδομένων προσωπικού χαρακτήρα.....	16
4α) Προσωπικά δεδομένα υπαλλήλων:	16
5) Δικαιώματα	16
6) Διαβίβαση δεδομένων σε τρίτους	17
7) Μέτρα ασφαλείας.....	18
8) Σύναψη συμφωνητικών εμπιστευτικότητας	19
9) Στοιχεία υπευθύνου προστασίας δεδομένων – Αρχής προστασίας δεδομένων	20
10) Επικοινωνία	20
<i>Πολιτική Ασφάλειας Επεξεργασίας Αρχείων.....</i>	<i>21</i>
<i>Εφαρμογή πολιτικής ασφάλειας.....</i>	<i>21</i>
1) Διαχείριση και Αποθήκευση Ψηφιακών Εγγράφων	21
Κανονική χρήση:.....	21
Αντικανονική Χρήση:.....	22
2) Υπηρεσίες Ηλεκτρονικού ταχυδρομείου	22
Κανονική χρήση:.....	22

Αντικανονική χρήση:	23
Υποχρεώσεις:.....	23
3) Διαδίκτυο	23
Αντικανονική χρήση	23
Υποχρεώσεις.....	24
4) Διαχείριση και αποθήκευση έντυπων εγγράφων.....	24
Κανονική χρήση:.....	24
Αντικανονική χρήση:	25

Προοίμιο

Το παρόν έγγραφο αποτελεί υποχρεωτικό κανονισμό για όλους τους υπάλληλους και συνεργάτες του Φορέα που συμμετέχουν, με οποιονδήποτε τρόπο, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή στη χρήση των πληροφοριακών συστημάτων του.

Σκοπός του είναι να καθορίσει σαφείς και δεσμευτικούς κανόνες συμπεριφοράς, πρακτικές ασφαλείας και υποχρεώσεις που απορρέουν από το ισχύον ευρωπαϊκό και εθνικό νομοθετικό πλαίσιο, καθώς και από τις εσωτερικές πολιτικές του Φορέα.

Ο Κανονισμός αυτός δεν υποκαθιστά τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ 2016/679), τον Ν. 4624/2019 ή άλλες σχετικές διατάξεις· αντιθέτως, λειτουργεί συμπληρωματικά ως πλαίσιο εφαρμογής των υποχρεώσεων που προκύπτουν από τη νομοθεσία και τις εσωτερικές διαδικασίες του Φορέα.

Όλοι οι υπάλληλοι και συνεργάτες οφείλουν να συμμορφώνονται πλήρως με τις προβλέψεις του παρόντος Κανονισμού κατά την εκτέλεση των καθηκόντων τους.

Η μη τήρηση των προβλέψεων αυτών ενδέχεται να επιφέρει υπηρεσιακές ή και νομικές συνέπειες, σύμφωνα με το εκάστοτε ισχύον πειθαρχικό και νομοθετικό πλαίσιο.

Ο Κανονισμός επικαιροποιείται περιοδικά ή όποτε απαιτείται, λόγω μεταβολών στη νομοθεσία, στις τεχνολογικές εξελίξεις ή στις εσωτερικές διαδικασίες του Φορέα.

Κάθε τροποποίηση τίθεται σε ισχύ από την ημερομηνία κοινοποίησής της και οι υπάλληλοι ενημερώνονται εγγράφως για τις αλλαγές.

Εισαγωγή

1) Γλωσσάριο - Συντομογραφίες

- **Φορέας:** Περιφερειακός Σύνδεσμος Φορέων Διαχείρισης Στερεών Αποβλήτων Κεντρικής Μακεδονίας
- **Γ.Κ.Π.Δ. ή G.D.P.R.:** Γενικός Κανονισμός Προστασίας Δεδομένων (Ε.Κ. 679/2016)
- **Υπεύθυνος επεξεργασίας:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που 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.
- **Διαχειριστής:** Ο υπάλληλος πληροφορικής, υπαγόμενος στο Τμήμα Πληροφορικής, Τηλεπικοινωνιών και Ασφάλειας Συστημάτων
- **E-mail:** Ηλεκτρονική αλληλογραφία
- **E-mail server:** Υπολογιστής ή υπολογιστές που φιλοξενεί/ούν την ηλεκτρονική αλληλογραφία των υπαλλήλων του Φορέα
- **E-mail client:** Πρόγραμμα που διαχειρίζεται την ηλεκτρονική αλληλογραφία
- **Πληροφοριακή υποδομή:** Το σύνολο των ηλεκτρονικών υπολογιστών που διαθέτει ο Φορέας, οι δικτυακές υποδομές, οι συνδέσεις στο διαδίκτυο, και οι λογαριασμοί ηλεκτρονικού ταχυδρομείου.
- **Υποκείμενο των δεδομένων:** Κάθε φυσικό πρόσωπο του οποίου τα προσωπικά δεδομένα υφίστανται επεξεργασία

2) Σκοπός

Ο παρών Κανονισμός αποσκοπεί στη θέσπιση δεσμευτικών κανόνων για την ασφαλή και ορθή χρήση των ηλεκτρονικών υπολογιστών, του διαδικτύου, του ηλεκτρονικού ταχυδρομείου και όλων των πληροφοριακών συστημάτων που παρέχει ο Φορέας στους υπαλλήλους και συνεργάτες του καθώς και για το φυσικό αρχείο.

Στόχος του είναι η διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα, η πρόληψη περιστατικών ασφάλειας και η πλήρης συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ 2016/679), τον Ν. 4624/2019 και τις εσωτερικές πολιτικές του Φορέα.

Ο Κανονισμός εφαρμόζεται υποχρεωτικά από όλους όσοι χρησιμοποιούν τα πληροφοριακά συστήματα του Φορέα ή συμμετέχουν σε οποιαδήποτε δραστηριότητα που περιλαμβάνει επεξεργασία δεδομένων προσωπικού χαρακτήρα.

3) Βασικές έννοιες και ορισμοί Γ.Κ.Π.Δ.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) έχει ως σκοπό την προστασία των φυσικών προσώπων από την παράνομη ή μη ορθή επεξεργασία των προσωπικών τους δεδομένων (άρθρο 1).

Ως «επεξεργασία» νοείται κάθε πράξη ή σειρά πράξεων που πραγματοποιείται, με ή χωρίς αυτοματοποιημένα μέσα, σε δεδομένα προσωπικού χαρακτήρα, όπως ενδεικτικά: συλλογή, καταχώριση, οργάνωση, αποθήκευση, μεταβολή, ανάκτηση, αναζήτηση, χρήση, κοινολόγηση, διάδοση, συσχέτιση, περιορισμός, διαγραφή ή καταστροφή (άρθρο 4 Γ.Κ.Π.Δ.).

Ως «παραβίαση δεδομένων» νοείται κάθε παραβίαση ασφάλειας που οδηγεί σε καταστροφή, απώλεια, μεταβολή, μη εξουσιοδοτημένη κοινολόγηση ή πρόσβαση (άρθρο 4 Γ.Κ.Π.Δ.).

4) Αρχές Νόμιμης Επεξεργασίας (Άρθρα 5 & 6 ΓΚΠΔ)

Για να είναι νόμιμη η επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρέπει να διενεργείται σύμφωνα με τις ακόλουθες αρχές:

α) Νομιμότητα, αντικειμενικότητα και διαφάνεια: Η επεξεργασία πρέπει να είναι νόμιμη, θεμιτή και διαφανής.

β) Περιορισμός του σκοπού: Συλλογή μόνο για συγκεκριμένους, σαφείς και νόμιμους σκοπούς.

γ) Ελαχιστοποίηση δεδομένων: Τα δεδομένα πρέπει να είναι απολύτως αναγκαία για τους σκοπούς επεξεργασίας.

δ) Ακρίβεια: Τα δεδομένα πρέπει να είναι ακριβή και επικαιροποιημένα.

ε) Ακεραιότητα και εμπιστευτικότητα: Εφαρμογή τεχνικών και οργανωτικών μέτρων ασφάλειας για προστασία από παράνομη επεξεργασία ή απώλεια.

στ) Περιορισμός περιόδου αποθήκευσης: Τήρηση μόνο για όσο χρόνο απαιτείται για τους σκοπούς επεξεργασίας.

ζ) Λογοδοσία: Ο Φορέας οφείλει να αποδεικνύει τη συμμόρφωσή του με όλες τις παραπάνω αρχές.

5) Ρόλος και Αρμοδιότητες του Τμήματος Πληροφορικής Τηλεπικοινωνιών και Ασφάλειας Συστημάτων

Το Τμήμα Πληροφορικής, Τηλεπικοινωνιών και Ασφάλειας Συστημάτων είναι αρμόδιο για τη σωστή και ασφαλή λειτουργία όλων των πληροφοριακών συστημάτων του Φορέα.

Στις αρμοδιότητές του περιλαμβάνονται μεταξύ άλλων:

- η επιτήρηση και διασφάλιση της ορθής λειτουργίας του δικτύου,
- η διαχείριση και προστασία των εξοπλισμών αποθήκευσης και επεξεργασίας δεδομένων (servers),
- η παρακολούθηση ειδοποιήσεων ασφαλείας και η λήψη μέτρων προστασίας στους δρομολογητές και λοιπές δικτυακές συσκευές,
- η εξασφάλιση της ασφαλούς λειτουργίας των τερματικών συσκευών του Φορέα.

Για την πρόληψη, ανίχνευση ή αντιμετώπιση περιστατικών ασφαλείας, το Τμήμα Πληροφορικής Τηλεπικοινωνιών και Ασφάλειας Συστημάτων δύναται να προβεί σε τοπική ή απομακρυσμένη πρόσβαση σε τερματικές συσκευές του Φορέα, χωρίς προηγούμενη ειδοποίηση του χρήστη, όταν αυτό είναι αναγκαίο (Για παράδειγμα: σε περίπτωση ειδοποίησης για απειλή από το σύστημα EDR {EDR=Εντοπισμός και Απόκριση σε Τερματικά Συστήματα} του Φορέα) για την προστασία της ασφαλείας των πληροφοριακών συστημάτων ή για τη διασφάλιση της ακεραιότητας των δεδομένων. Κάθε τέτοια πρόσβαση τεκμηριώνεται υποχρεωτικά σε ειδικό αρχείο καταγραφής.

Σε περίπτωση ελέγχου από αρμόδιες αρχές, το Τμήμα Πληροφορικής Τηλεπικοινωνιών και Ασφάλειας Συστημάτων οφείλει να παρέχει κάθε πληροφορία ή τεχνική υποστήριξη που απαιτείται για τη διερεύνηση του περιστατικού.

6) Κυρώσεις σε Περίπτωση Μη Συμμόρφωσης

Σε περίπτωση μη συμμόρφωσης του Φορέα με τα απαιτούμενα μέτρα ασφαλείας, τις διαδικασίες προστασίας δεδομένων ή τις λοιπές υποχρεώσεις που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ), προβλέπονται ιδιαίτερα αυστηρές κυρώσεις.

Σύμφωνα με τα άρθρα 82–84 του ΓΚΠΔ, οι κυρώσεις μπορεί να περιλαμβάνουν:

- Διοικητικά πρόστιμα έως 20.000.000 € ή έως 4% του συνολικού ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (ανάλογα με το ποιο ποσό είναι υψηλότερο).
- Αστικές αξιώσεις για αποζημίωση από τα υποκείμενα των δεδομένων.

- Ποινικές ή άλλες διοικητικές κυρώσεις, όπου αυτές προβλέπονται από την εθνική νομοθεσία.

Οι κυρώσεις μπορεί να επιβληθούν τόσο στον Υπεύθυνο Επεξεργασίας όσο και στον Εκτελούντα την Επεξεργασία, ανεξάρτητα από το αν έχει προκύψει αποδεδειγμένη διαρροή δεδομένων· αρκεί να διαπιστωθεί ότι υπήρξε παράβαση των υποχρεώσεων που επιβάλλει ο Κανονισμός.

Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Εισαγωγή

Ο Περιφερειακός Σύνδεσμος Φορέων Διαχείρισης Στερεών Αποβλήτων Κεντρικής Μακεδονίας ΝΠΔΔ (ΦΕΚ Σύστασης 1908Β/2012) (στο εξής: Φορέας) δίνει ιδιαίτερη σημασία στην προστασία της ιδιωτικότητας, του απορρήτου και της εμπιστευτικότητας των προσωπικών δεδομένων που επεξεργάζεται στο πλαίσιο της λειτουργίας του. Για το σκοπό αυτό εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας, επενδύει σε υποδομές και εκπαίδευση, και βρίσκεται σε διαρκή διαδικασία ενημέρωσης και συμμόρφωσης με το ισχύον εθνικό και ευρωπαϊκό νομικό πλαίσιο και ιδίως με το Γενικό Κανονισμό Προστασίας των Δεδομένων (στο εξής: Γ.Κ.Π.Δ.) Προσωπικού Χαρακτήρα 2016/679 της Ευρωπαϊκής Ένωσης και τον ελληνικό εφαρμοστικό του νόμο Ν. 4624/2019. Είναι σημαντικό να σημειωθεί ότι ο Κανονισμός εφαρμόζεται αποκλειστικά στα δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων και όχι σε δεδομένα νομικών προσώπων.

1) Σκοπός

Με την παρούσα πολιτική προστασίας δεδομένων προσωπικού χαρακτήρα (στο εξής: «Πολιτική»), ο Φορέας επιδιώκει να ενημερώσει με διαφάνεια τα υποκείμενα των δεδομένων για:

- τον τρόπο με τον οποίο συλλέγουμε, αποθηκεύουμε, χρησιμοποιούμε και διαβιβάζουμε τα δεδομένα προσωπικού χαρακτήρα,
- τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουμε για την προστασία τους,
- τους σκοπούς και τη διάρκεια τήρησης των δεδομένων, καθώς και τα κριτήρια που καθορίζουν τον χρόνο διατήρησής τους,
- το είδος των δεδομένων που συλλέγουμε στο πλαίσιο των δραστηριοτήτων μας.

Η Πολιτική καλύπτει κάθε πράξη επεξεργασίας δεδομένων προσωπικού χαρακτήρα κατά την έννοια του άρθρου 4 του Γενικού Κανονισμού (ΕΕ) 2016/679, όπως είναι ενδεικτικά η συλλογή, η αποθήκευση, η χρήση, η διαβίβαση, η διάδοση, η συσχέτιση, ο περιορισμός, η διαγραφή ή η καταστροφή.

2) Τί είναι τα δεδομένα προσωπικού χαρακτήρα

Είναι κάθε πληροφορία που αφορά ένα συγκεκριμένο φυσικό πρόσωπο, του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί άμεσα ή έμμεσα. Ενδεικτικά αναφέρονται: όνομα, επώνυμο, αριθμός ταυτότητας ή διαβατηρίου, στοιχεία επικοινωνίας, διεύθυνση κατοικίας, στοιχεία οικονομικής ταυτότητας, αλλά και οποιαδήποτε πληροφορία σχετίζεται με τα χαρακτηριστικά, τις δραστηριότητες ή την κατάσταση του προσώπου. Στον γενικό αυτόν ορισμό περιλαμβάνονται και τα **ειδικών κατηγοριών δεδομένα** (άρθρο 9 GDPR), δηλαδή δεδομένα που αφορούν:

- την υγεία (σωματική ή ψυχική),
- τη λήψη ιατρικών υπηρεσιών,
- τη γενετική ή βιομετρική ταυτότητα,
- τις θρησκευτικές ή πολιτικές πεποιθήσεις,
- τη φυλετική ή εθνική καταγωγή,
- τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό.

Τα δεδομένα αυτά χρήζουν αυξημένης προστασίας και επεξεργάζονται μόνο όταν συντρέχουν οι νόμιμες προϋποθέσεις που ορίζει ο Γ.Κ.Π.Δ. και ο Ν. 4624/2019.

Ο Φορέας εφαρμόζει αυστηρά την **αρχή της ελαχιστοποίησης των δεδομένων** (άρθρο 5 GDPR). Αυτό σημαίνει ότι:

- συλλέγει και επεξεργάζεται **μόνο τα απολύτως απαραίτητα** δεδομένα που απαιτούνται για τον σκοπό για τον οποίο προορίζονται,
- απέχει από τη συλλογή πλεονάζουσας ή μη συναφούς πληροφορίας,
- συμμορφώνεται πλήρως με τις προϋποθέσεις και τα όρια που θέτει ο Ν. 4624/2019 και το ισχύον κανονιστικό πλαίσιο.

3) Συλλογή

3α) Τρόποι Συλλογής Δεδομένων

Η συλλογή δεδομένων προσωπικού χαρακτήρα πραγματοποιείται με νόμιμο και διαφανή τρόπο, σύμφωνα με τον Γ.Κ.Π.Δ. και τον Ν. 4624/2019. Ειδικότερα:

- Τα έγγραφα που περιέχουν δεδομένα προσωπικού χαρακτήρα **παραλαμβάνονται από το Τμήμα Πρωτοκόλλου**, είτε σε **έντυπη** είτε σε **ψηφιακή μορφή**.
- Η συλλογή μπορεί να πραγματοποιείται επίσης μέσω:
 - ηλεκτρονικής αλληλογραφίας,
 - υποβολής αιτήσεων και δικαιολογητικών
 - υπηρεσιακών πληροφοριακών συστημάτων

- διαλειτουργικότητας με άλλους δημόσιους φορείς σύμφωνα με το ισχύον νομικό πλαίσιο.

Ο Φορέας συλλέγει μόνο τα δεδομένα που είναι **απαραίτητα** για την άσκηση των αρμοδιοτήτων του και την ορθή λειτουργία των υπηρεσιών του («αρχή της ελαχιστοποίησης των δεδομένων»).

3β) Ποια δεδομένα συλλέγονται:

Για τους υπαλλήλους του Φορέα συλλέγονται τα απολύτως αναγκαία δεδομένα προσωπικού χαρακτήρα, τα οποία απαιτούνται για:

- την πρόσληψη και τήρηση υπηρεσιακού φακέλου,
- τη μισθοδοσία και ασφαλιστική τους κάλυψη,
- την ομαλή υπηρεσιακή τους απασχόληση,
- την προστασία της υγείας και ασφάλειας στην εργασία,
- τη συνταξιοδότησή τους.

Αναλυτικότερα, τα δεδομένα που συλλέγονται κατά την έκδοση της παρούσης είναι (ενδεικτικά και όχι περιοριστικά) τα εξής:

i. Στοιχεία Ταυτοποίησης και Επικοινωνίας

- Ονοματεπώνυμο
- Πατρώνυμο
- Μητρώνυμο
- Αριθμοί τηλεφώνου
- Αριθμός δελτίου αστυνομικής ταυτότητας
- Προσωπικός αριθμός υπαλλήλου
- Διεύθυνση κατοικίας

ii. Διοικητικά, Μισθολογικά και Ασφαλιστικά Στοιχεία

- Αριθμός Φορολογικού Μητρώου (Α.Φ.Μ.)
- Αριθμός Μητρώου Κοινωνικής Ασφάλισης (Α.Μ.Κ.Α.)
- Αριθμός τραπεζικού λογαριασμού (IBAN)
- Στοιχεία πρότερου ασφαλιστικού βίου
- Εκκαθαριστικό εφορίας (σε περιπτώσεις που απαιτείται από την υπηρεσία)

iii. Στοιχεία Επαγγελματικής Κατάστασης και Προσόντων

- Τίτλοι σπουδών
- Δικαιολογητικά πιστοποίησης επαγγελματικών προσόντων

iv. Ποινικά και Δικαστικά Δεδομένα (όπου απαιτείται από τη νομοθεσία)

- Απόσπασμα ποινικού μητρώου

Σημ.: Τα δεδομένα αυτά ανήκουν σε ειδική κατηγορία επεξεργασίας και συλλέγονται μόνο όταν προβλέπεται ρητά από τον νόμο.

v. Δεδομένα Υγείας (Ειδικές Κατηγορίες Δεδομένων – Άρθρο 9 Γ.Κ.Π.Δ.)

Συλλέγονται μόνο όταν είναι απαραίτητα για την άσκηση των καθηκόντων του Φορέα και την προστασία της υγείας και ασφάλειας των εργαζομένων:

- Πιστοποιητικό υγείας για την επαγγελματική ικανότητα
- Αποτελέσματα ιατρικών εξετάσεων, όταν απαιτείται από ιατρό εργασίας ή ειδική νομοθεσία
- Αποφάσεις αναπηρίας (σε περίπτωση που σχετίζονται με άδειες, παροχές ή δικαιώματα)

vi. Δεδομένα που περιλαμβάνονται σε υποβληθέντα δικαιολογητικά και έγγραφα

Έγγραφα που συχνά περιέχουν προσωπικά δεδομένα των υπαλλήλων ή μελών της οικογένειάς τους, όπως:

- Υπεύθυνη δήλωση (άρθρο 8 Ν. 1599/1986)
- Πιστοποιητικό οικογενειακής κατάστασης
- Πιστοποιητικό γέννησης
- Πιστοποιητικό θανάτου
- Πιστοποιητικό γάμου ή σύμφωνο συμβίωσης
- Πιστοποιητικό βάφτισης (όπου απαιτείται για τέκνα)

vi. Δεδομένα που περιλαμβάνονται σε ψηφιακές βάσεις δεδομένων του ελληνικού δημοσίου

Το σύνολο των προσωπικών δεδομένων που είναι διαθέσιμα στις ψηφιακές βάσεις δεδομένων του ελληνικού κράτους (ενδεικτικά και όχι περιοριστικά αναφέρονται: Εθνικό Μητρώο Επικοινωνίας, e-ΕΦΚΑ, myAADE) είναι προσβάσιμα από το Τμήμα Διαχείρισης Ανθρωπίνου Δυναμικού & Μισθοδοσίας του Φορέα.

Για τους αναδόχους ή τους υποψήφιους αναδόχους δημοσίων συμβάσεων που συνάπτει ο Φορέας, συλλέγονται όλα τα απαραίτητα δεδομένα προσωπικού χαρακτήρα που απαιτούνται για:

- την υποβολή προσφοράς,
- την αξιολόγηση και ανάθεση έργου, προμήθειας ή υπηρεσίας,
- την παρακολούθηση και επιτήρηση της υλοποίησης της σύμβασης,
- την παραλαβή των παραδοτέων,
- την οικονομική τακτοποίηση και αποπληρωμή.

Η συλλογή των δεδομένων πραγματοποιείται σύμφωνα με το ισχύον νομικό πλαίσιο περί δημοσίων συμβάσεων και τις αρχές του GDPR. Αναλυτικότερα, τα δεδομένα

που συλλέγονται κατά την έκδοση της παρούσης είναι (ενδεικτικά και όχι περιοριστικά) τα εξής:

I. Στοιχεία Ταυτοποίησης Προσώπων που συμμετέχουν στη διαδικασία

- Ονοματεπώνυμο
- Πατρώνυμο
- Μητρώνυμο
- Αριθμός δελτίου αστυνομικής ταυτότητας νομίμου εκπροσώπου ή μελών της διοίκησης της εταιρείας ή άλλων προσώπων που υποβάλλουν την οικονομική προσφορά
- Διεύθυνση έδρας επιχείρησης
- Αριθμός τηλεφώνου
- E-mail

II. Φορολογικά, Ασφαλιστικά και Οικονομικά Δεδομένα

- Αριθμός Φορολογικού Μητρώου (Α.Φ.Μ.)
- Αριθμός Μητρώου Κοινωνικής Ασφάλισης (Α.Μ.Κ.Α.)
- Αριθμός τραπεζικού λογαριασμού (IBAN)
- Πιστοποιητικό φορολογικής ενημερότητας
- Πιστοποιητικό ασφαλιστικής ενημερότητας
- Ετήσιος κύκλος εργασιών για συγκεκριμένη περίοδο
- Οικονομικά στοιχεία άλλων συμβάσεων της επιχείρησης με δημόσιους φορείς
- Πληροφορίες για τυχόν ασφαλιστική κάλυψη επαγγελματικών κινδύνων

III. Νομικά Έγγραφα και Πιστοποιήσεις Επιχειρηματικής Ικανότητας

- Καταστατικό σύστασης ή τροποποιήσεις αυτού
- Πιστοποιητικό εγγραφής σε Επιμελητήριο (Γ.Ε.ΜΗ.)
- Έναρξη εργασιών στη Δ.Ο.Υ.
- Βεβαίωση μη παύσης εργασιών
- Πιστοποιητικά περί μη υπαγωγής σε πτωχευτική ή προπτωχευτική διαδικασία
- Αναλυτικό πιστοποιητικό εκπροσώπησης
- Ιστορικό επαγγελματικής δραστηριότητας

IV. Στοιχεία Τεχνικής & Επαγγελματικής Ικανότητας

- Τίτλοι σπουδών
- Πιστοποιητικά εμπειρίας
- Στοιχεία τεχνικής καταλληλότητας
- Αριθμός κυκλοφορίας οχημάτων της επιχείρησης (όπου απαιτείται για την τεχνική αξιολόγηση ή εκτέλεση έργου)

V. Ποινικά Δεδομένα (όπου το απαιτεί η νομοθεσία δημοσίων συμβάσεων)

- Απόσπασμα ποινικού μητρώου μελών διοικητικού ή/και εποπτικού οργάνου, διευθύνοντος συμβούλου, διαχειριστών ή νομίμων εκπροσώπων, σύμφωνα με την ισχύουσα νομοθεσία.

Σημ.: Η συλλογή ποινικών δεδομένων προβλέπεται από το θεσμικό πλαίσιο δημοσίων συμβάσεων (Ν. 4412/2016 και επόμενες τροποποιήσεις) και επιτρέπεται μόνο υπό τις προϋποθέσεις του άρθρου 10 GDPR.

Παροχή πρόσθετων δεδομένων εκ μέρους προσφερόντων

Σε περίπτωση που ο προσφέρων οικονομικός φορέας, ο ανάδοχος ή τρίτος εμπλεκόμενος στη σύμβαση υποβάλει δικαιολογητικά που περιέχουν **επιπλέον** κατηγορίες δεδομένων προσωπικού χαρακτήρα — απλών ή ειδικών κατηγοριών — πέρα από όσα προβλέπονται στην παρούσα ενότητα:

- Τα δεδομένα αυτά παρέχονται **οικειοθελώς** από τα υποκείμενα.
- Θεωρείται ότι παρέχονται **με τη ρητή τους συγκατάθεση**, εφόσον δεν ζητούνται από τον Φορέα.
- Ο Φορέας τα επεξεργάζεται **μόνο εφόσον είναι αναγκαία** για την εκτέλεση ή παρακολούθηση της σύμβασης ή όταν αυτό επιβάλλεται από τη σχετική νομοθεσία.

3γ) Για ποιους λόγους συλλέγονται/Νομική βάση

Η λειτουργία του φορέα βασίζεται στον νόμο Ν. 3463/2006, Ν.3852/2010 και Ν. 4555/2018 ως ισχύουν σήμερα με τις τροποποιήσεις τους.

Για τα τεχνικά έργα, τις προμήθειες και τις υπηρεσίες που υλοποιεί ο φορέας βασίζονται στο Ν. 4412/2016 ως ισχύει.

Το Τμήμα Ανθρωπίνου Δυναμικού βασίζεται στους νόμους, Ν. 3528/2007, 3584/2007 κώδικας δημοσίων υπαλλήλων (αρμοδιότητες και καθήκοντα) ως ισχύουν σήμερα με τις τροποποιήσεις τους.

Επίσης ενδεικτικά εφαρμόζονται οι:

- Ν. 4305/2014 άρθρο 28, όπως ισχύει με τις τροποποιήσεις με το άρθρο 26 Ν. 4440/2016, για τη γνησιότητα των εγγράφων και τα γνήσια αντίγραφα.
- Ν. 4210/2013 άρθρο 7, Ν. 3584/2007 άρθρο 14 όπως ισχύει με τις τροποποιήσεις με το άρθρο 48 Ν. 4674/2020, αφορούν την σωματική και ιατρική ικανότητα του εργαζομένου των εργαζομένων στο Δημόσιο Τομέα.
- Ν.4354/2015 όπως ισχύει με τις τροποποιήσεις του, αφορά τα μισθολογικά ζητήματα των εργαζομένων στο Δημόσιο Τομέα.
- Ν. 3584/2007, άρθρο 16 για το πιστοποιητικό ποινικού μητρώου των εργαζομένων στο Δημόσιο Τομέα.

4) Χρόνος τήρησης των δεδομένων προσωπικού χαρακτήρα

4α) Προσωπικά δεδομένα υπαλλήλων:

Από την ίδρυσή του το 2014 μέχρι και σήμερα ο Φορέας δεν έχει προβεί σε διαγραφή δεδομένων υπαλλήλων, καθώς μεγάλο μέρος των δεδομένων αυτών εμπίπτει σε κατηγορίες που η ισχύουσα νομοθεσία επιβάλλει την πολυετή ή και διαχρονική τήρησή τους (υπηρεσιακά στοιχεία, μισθολογικά, ασφαλιστικά, διοικητικές πράξεις κ.λπ.).

Ο Φορέας βρίσκεται ήδη στη διαδικασία κατάρτισης Πολιτικής Χρόνου Διατήρησης Δεδομένων, με σκοπό τον σαφή καθορισμό και την τεκμηριωμένη εφαρμογή χρόνων τήρησης για όλες τις κατηγορίες δεδομένων.

Σε περίπτωση που επιθυμείτε κάποιο/α από τα δεδομένα σας να διαγραφούν, μπορείτε να ασκήσετε το δικαίωμα της διαγραφής όπως περιγράφεται στο άρθρο 5 της παρούσης πολιτικής. Ο Φορέας θα εξετάσει τη νομιμότητα του αιτήματος κατά την τρέχουσα εθνική και ευρωπαϊκή νομοθεσία και θα σας απαντήσει εγγράφως εντός ενός (1) μηνός είτε για την επιβεβαίωση της διαγραφής είτε για την αιτιολογημένη άρνηση της.

5) Δικαιώματα

Για όσο χρόνο ο Φορέας διατηρεί τα δεδομένα προσωπικού χαρακτήρα, έχετε τα ακόλουθα δικαιώματα σύμφωνα με τα άρθρα 12 - 22 του Γ.Κ.Π.Δ.:

- **Δικαίωμα πρόσβασης:** Δικαιούστε να ενημερωθείτε αν ο Φορέας επεξεργάζεται τα προσωπικά σας δεδομένα και, εφόσον ισχύει, να λάβετε πρόσβαση σε αυτά και σε πληροφορίες σχετικά με την επεξεργασία τους.
- **Δικαίωμα διόρθωσης:** Μπορείτε να ζητήσετε τη διόρθωση ή συμπλήρωση ανακριβών ή ελλιπών δεδομένων σας. Η διόρθωση ισχύει για κάθε επεξεργασία που λαμβάνει χώρα μετά τη γνωστοποίησή της στον Φορέα.
- **Δικαίωμα διαγραφής:** Έχετε δικαίωμα να αιτηθείτε τη διαγραφή των δεδομένων σας. Ο Φορέας συλλέγει και επεξεργάζεται μόνο τα απολύτως απαραίτητα δεδομένα· συνεπώς, εντός ενός (1) μηνός από τη λήψη του αιτήματος, θα ενημερωθείτε:
 - για το αν η διαγραφή μπορεί να πραγματοποιηθεί,
 - ποιες υπηρεσιακές λειτουργίες θα επηρεαστούν και
 - αν υφίσταται νομική υποχρέωση που επιβάλλει τη διατήρησή τους.

Εφόσον πληρούνται οι προϋποθέσεις του νόμου, η διαγραφή θα εκτελεστεί και θα ενημερωθείτε εγγράφως.

- **Δικαίωμα στις διαβιβάσεις δεδομένων (φορητότητα):** Μπορείτε να ζητήσετε τη διαβίβαση των δεδομένων σας σε άλλον υπεύθυνο επεξεργασίας, όπου αυτό είναι τεχνικά εφικτό και επιτρεπτό από τη νομοθεσία.
 - Σε περίπτωση αδυναμίας εκπλήρωσης του αιτήματος, ο Φορέας θα σας παράσχει εγγράφως αιτιολογημένη απάντηση.
 - **Δικαίωμα καταγγελίας στην εποπτική αρχή:** Έχετε δικαίωμα να υποβάλετε καταγγελία στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), εάν θεωρείτε ότι η επεξεργασία των δεδομένων σας παραβιάζει το ισχύον πλαίσιο προστασίας προσωπικών δεδομένων.
- Περισσότερες πληροφορίες παρατίθενται στο άρθρο 9 της παρούσας πολιτικής.

6) Διαβίβαση δεδομένων σε τρίτους

Σε προγραμματισμένη βάση ή όταν αυτό απαιτηθεί, ο Φορέας δύναται να διαβιβάζει τα απολύτως αναγκαία δεδομένα προσωπικού χαρακτήρα που τηρεί, σε υπηρεσίες και δομές της δημόσιας διοίκησης, συμπεριλαμβανομένων φορέων του στενού και του ευρύτερου δημόσιου τομέα.

Οι διαβιβάσεις αυτές πραγματοποιούνται αποκλειστικά για την εκτέλεση των νόμιμων αρμοδιοτήτων του Φορέα, σύμφωνα με το άρθρο 6(1)(γ) και 6(1)(ε) του Γ.Κ.Π.Δ., καθώς και τις προϋποθέσεις του άρθρου 24 του Ν. 4624/2019. Δεδομένου ότι η διαβίβαση στηρίζεται σε νομική υποχρέωση ή αφορά εκπλήρωση καθήκοντος που ασκείται προς το δημόσιο συμφέρον, και εφόσον πληρούνται οι προϋποθέσεις του άρθρου 26 του Ν. 4624/2019, δεν απαιτείται η συναίνεση του υποκειμένου των δεδομένων, ούτε απαιτείται εκ νέου ενημέρωση πέραν αυτής που παρέχεται μέσω της παρούσας πολιτικής.

Ενδεικτικά και όχι περιοριστικά αναφέρονται οι κάτωθι:

- Ε.Φ.Κ.Α. - Ι.Κ.Α.
- Δ.Υπ.Α.
- Επιθεώρηση Εργασίας
- Υπουργεία Δικαιοσύνης, Εσωτερικών και Οικονομικών και σε υπηρεσίες των υπουργείων αυτών
- Ελεγκτικό συνέδριο

- Γενικό λογιστήριο του κράτους (Ενιαία Αρχή Πληρωμών και υπηρεσία συντάξεων)
- Λοιπούς φορείς της Γενικής Κυβέρνησης, όταν αυτό προβλέπεται από το ισχύον θεσμικό πλαίσιο

7) Μέτρα ασφαλείας

Ο Φορέας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας με σκοπό την προστασία των δεδομένων προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη πρόσβαση, χρήση ή δημοσιοποίηση.

Τα μέτρα αυτά επανεξετάζονται και επικαιροποιούνται όποτε απαιτείται, σύμφωνα με τις αρχές του άρθρου 32 του GDPR.

Ενδεικτικά, εφαρμόζονται τα ακόλουθα:

Α) Μέτρα ασφαλείας για το φυσικό (έντυπο) αρχείο

- ✓ Τήρηση μέρους του αρχείου και σε ηλεκτρονική μορφή για λόγους ασφαλούς διαχείρισης και αντιγράφων.
- ✓ Περιορισμένη πρόσβαση προσωπικού στους χώρους φύλαξης φυσικών αρχείων
- ✓ Ασφάλιση των χώρων μέσω κλειδώματος γραφείων και ελεγχόμενης πρόσβασης.
- ✓ Επίβλεψη συγκεκριμένων χώρων μέσω συστημάτων καμερών ασφαλείας, όπου αυτό επιτρέπεται από την κείμενη νομοθεσία.

Β) Μέτρα ασφαλείας για τα ψηφιακά αρχεία και πληροφοριακά συστήματα

- ✓ Χρήση τείχους προστασίας (firewall) για την αποτροπή μη εξουσιοδοτημένης πρόσβασης από το διαδίκτυο.
- ✓ Εφαρμογή πρωτοκόλλων κρυπτογράφησης (όπως SSL/TLS) για την ασφαλή μεταφορά δεδομένων μεταξύ χρηστών και συστημάτων του Φορέα.
- ✓ Χρήση ισχυρών κωδικών πρόσβασης σε όλους τους υπολογιστές και εφαρμογές που επεξεργάζονται ή αποθηκεύουν δεδομένα προσωπικού χαρακτήρα.
- ✓ Κρυπτογράφηση δίσκων ή αρχείων που περιέχουν δεδομένα προσωπικού χαρακτήρα.

- ✓ Τακτική δημιουργία αντιγράφων ασφαλείας (backups) αρχείων και βάσεων δεδομένων, σε καθημερινή ή εβδομαδιαία βάση, ανάλογα με τον τύπο και την κρισιμότητά τους.
- ✓ Η ιστοσελίδα του Φορέα έχει σχεδιαστεί με βάση σύγχρονες τεχνολογίες και πρακτικές που ενισχύουν την ασφάλεια, την απόδοση και τη λειτουργικότητά της.

Γ) Οργανωτικά μέτρα ασφαλείας

- ✓ Περιορισμός πρόσβασης στα δεδομένα μόνο σε εξουσιοδοτημένο προσωπικό, ανάλογα με τον ρόλο και τα καθήκοντά του.
- ✓ Τεκμηριωμένες διαδικασίες και πολιτικές για την ορθή επεξεργασία, αποθήκευση και διαβίβαση προσωπικών δεδομένων.
- ✓ Εκπαίδευση και ενημέρωση προσωπικού σχετικά με την προστασία δεδομένων, τα καθήκοντά τους και τις υποχρεώσεις εμπιστευτικότητας.
- ✓ Περιοδικός έλεγχος και επικαιροποίηση των πολιτικών και διαδικασιών ασφαλείας.
- ✓ Καθορισμός υπευθύνων για τη διαχείριση θεμάτων ασφάλειας και προστασίας δεδομένων.
- ✓ Τήρηση πολιτικής πρόσβασης και διαβαθμισμένων δικαιωμάτων, με τακτικό έλεγχο και ανανέωση των κωδικών.

8) Σύναψη συμφωνητικών εμπιστευτικότητας

Οι συνεργασίες του Φορέα με εξωτερικούς συνεργάτες που - επιβεβαιωμένα ή δυνητικά - έρχονται σε επαφή με δεδομένα προσωπικού χαρακτήρα διέπονται από συμφωνητικά εμπιστευτικότητας σύμφωνα με τα άρθρα 28 και 29 του Γ.Κ.Π.Δ..

Τα συμφωνητικά αυτά καθορίζουν:

- ✓ την υποχρέωση εμπιστευτικότητας των συνεργατών,
- ✓ τα μέτρα ασφαλείας που οφείλουν να τηρούν,
- ✓ τους περιορισμούς πρόσβασης στα δεδομένα,
- ✓ την απαγόρευση μη εξουσιοδοτημένης χρήσης ή διαβίβασης,

- ✓ τις υποχρεώσεις συμμόρφωσης με την πολιτική του Φορέα και το ισχύον νομικό πλαίσιο προστασίας δεδομένων.

Ο Φορέας διασφαλίζει ότι κάθε εξωτερικός συνεργάτης που επεξεργάζεται δεδομένα για λογαριασμό του ενεργεί μόνο βάσει εντολών του Φορέα και σύμφωνα με τα προβλεπόμενα στην παρούσα πολιτική.

9) Στοιχεία υπευθύνου προστασίας δεδομένων – Αρχής προστασίας δεδομένων

Για οποιαδήποτε απορία σχετικά με την επεξεργασία των προσωπικών σας δεδομένων από τον Φορέα ή για θέματα άσκησης των δικαιωμάτων σας σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 και την ελληνική νομοθεσία, μπορείτε να επικοινωνείτε με τον Υπεύθυνο Προστασίας Δεδομένων (DPO) του Φορέα στο e-mail: dpo@fodsakm.gr

Ο Υπεύθυνος Προστασίας Δεδομένων του Φορέα είναι ο κ. Καρακατσάνης Πολύκαρπος

Σε περίπτωση που θεωρείτε ότι η επεξεργασία των δεδομένων σας παραβιάζει το ισχύον πλαίσιο προστασίας προσωπικών δεδομένων, έχετε δικαίωμα να υποβάλετε καταγγελία στην αρμόδια εποπτική αρχή:

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Ιστότοπος: www.dpa.gr

Τηλεφωνικό κέντρο: +30 210 6475600

Ηλεκτρονικό ταχυδρομείο: contact@dpa.gr

10) Επικοινωνία

Ο Περιφερειακός Σύνδεσμος ΦΟΔΣΑ Κεντρικής Μακεδονίας εδρεύει στον Δήμο Θεσσαλονίκης, στη διεύθυνση Φράγκων 6–8, Τ.Κ. 54626.

Για γενικές πληροφορίες και αιτήματα, μπορείτε να επικοινωνείτε στο +30 2311 236100.

Το τηλεφωνικό κέντρο λειτουργεί καθημερινά, από Δευτέρα έως Παρασκευή, και ώρες 07:00 π.μ. – 15:00 μ.μ.

Η διεύθυνση ηλεκτρονικού ταχυδρομείου επικοινωνίας είναι: info@fodsakm.gr

Πολιτική Ασφάλειας Επεξεργασίας Αρχείων

Εφαρμογή πολιτικής ασφάλειας

Η παρούσα Πολιτική Ασφάλειας εφαρμόζεται υποχρεωτικά σε όλα τα άτομα, συστήματα και δεδομένα που εμπίπτουν στη λειτουργία του Φορέα. Ειδικότερα, η εφαρμογή της καλύπτει:

α) Χρήστες

- Όλους τους υπαλλήλους του Φορέα, ανεξαρτήτως σχέσης εργασίας.
- Τους εξωτερικούς συνεργάτες, προμηθευτές ή τεχνικούς που αποκτούν πρόσβαση στο δίκτυο ή στις υπηρεσιακές εφαρμογές.
- Τους περιστασιακούς χρήστες που αποκτούν προσωρινή ή περιορισμένη πρόσβαση στα συστήματα του Φορέα.

β) Δεδομένα και αρχεία

- Όλα τα αρχεία και δεδομένα που δημιουργούνται, λαμβάνονται, αποθηκεύονται ή επεξεργάζονται από τους υπαλλήλους στο πλαίσιο της υπηρεσιακής τους δραστηριότητας.
- Όλα τα αρχεία που λαμβάνονται μέσω ηλεκτρονικού ταχυδρομείου, τόσο από υπηρεσιακούς λογαριασμούς όσο και από συνεργάτες, προμηθευτές ή τρίτους φορείς.

γ) Πληροφοριακά συστήματα και εξοπλισμός

- Όλα τα συστήματα ηλεκτρονικής αλληλογραφίας που παρέχονται από τον Φορέα.
- Όλες τις τερματικές συσκευές, υπολογιστές, φορητές συσκευές και άλλον εξοπλισμό που χρησιμοποιείται για υπηρεσιακούς σκοπούς.
- Το δίκτυο, τους διακομιστές και κάθε υποδομή πληροφορικής του Φορέα.

δ) Πρόσβαση σε διαδικτυακούς πόρους

- Όλους τους ιστότοπους και ηλεκτρονικούς πόρους που χρησιμοποιούνται στο πλαίσιο των υπηρεσιακών καθηκόντων.
- Online υπηρεσίες, πλατφόρμες και εφαρμογές που σχετίζονται με το έργο και τις δραστηριότητες του Φορέα.

1) Διαχείριση και Αποθήκευση Ψηφιακών Εγγράφων

Κανονική χρήση:

Οι υπάλληλοι οφείλουν να αποθηκεύουν τα ηλεκτρονικά έγγραφα αποκλειστικά στους προβλεπόμενους υπηρεσιακούς φακέλους, ανάλογα με τη φύση τους:

- **Προσωπικά υπηρεσιακά έγγραφα:** Αποθηκεύονται στον προσωπικό φάκελο του υπαλλήλου, στον οποίο έχει πρόσβαση μόνο ο ίδιος.
- **Έγγραφα Τμήματος:** Αποθηκεύονται στον φάκελο του αρμόδιου Τμήματος, στον οποίο έχουν πρόσβαση μόνο τα εξουσιοδοτημένα μέλη του Τμήματος.
- **Έγγραφα Διεύθυνσης:** Αποθηκεύονται στον φάκελο της Διεύθυνσης, με πρόσβαση περιορισμένη σε εξουσιοδοτημένους υπαλλήλους.

- **Εισερχόμενα έγγραφα:** Αποθηκεύονται αποκλειστικά στους αντίστοιχους φακέλους της Διεύθυνσης ή του Τμήματος, ώστε να διασφαλίζεται η εύκολη αναζήτηση και η ενιαία αρχειοθέτηση.

Η εφαρμογή της πρακτικής αυτής διασφαλίζει:

- **Εμπιστευτικότητα** (πρόσβαση μόνο από εξουσιοδοτημένα άτομα),
- **Ακεραιότητα** (έλεγχος αλλαγών και σωστή έκδοση αρχείων),
- **Διαθεσιμότητα** (λήψη αντιγράφων ασφαλείας σε καθημερινή βάση).

Αντικανονική Χρήση:

Αντικανονική χρήση αποτελεί:

- Η αποθήκευση υπηρεσιακών αρχείων **τοπικά** στους υπολογιστές.
- Η αποθήκευση σε εξωτερικά μέσα (CD, USB, εξωτερικούς δίσκους) **χωρίς έγκριση** του Τμήματος Πληροφορικής.
- Η αποθήκευση σε **μη εγκεκριμένες υπηρεσίες cloud** (π.χ. προσωπικά Google Drive, Dropbox, OneDrive).
- Η **μη εξουσιοδοτημένη** διαγραφή, αντιγραφή ή αποστολή αρχείων.
- Η εγκατάσταση/χρήση λογισμικών χωρίς έγκριση του Τμήματος Πληροφορικής.
- Η χρήση εργαλείων διαμοιρασμού (torrents, magnets κ.λπ.).
- Η μεταφόρτωση αρχείων άσχετων με τα υπηρεσιακά καθήκοντα ή από μη ασφαλείς πηγές.

2) Υπηρεσίες Ηλεκτρονικού ταχυδρομείου

Οι λογαριασμοί ηλεκτρονικών ταχυδρομείων της υπηρεσίας ανήκουν στο φορέα και δεν είναι προσωπικοί. Ο φορέας παρέχει αυτές τις ηλεκτρονικές υπηρεσίες με σκοπό την υποστήριξη των οργανικών του μονάδων.

Κανονική χρήση:

Οι χρήστες:

- Οφείλουν να χρησιμοποιούν το email σύμφωνα με τη νομοθεσία, την πολιτική ασφάλειας και την αρχή της εμπιστευτικότητας.
- Πρέπει να αποθηκεύουν σημαντικά συνημμένα στους αντίστοιχους φακέλους δικτύου (ο Φορέας **δεν** τηρεί ξεχωριστό αρχείο e-mail για αυτούς).
- Οφείλουν να προστατεύουν συνημμένα που περιέχουν προσωπικά δεδομένα (**όχι προώθηση σε προσωπικά emails, όχι αποθήκευση σε μη εγκεκριμένα μέσα**).

Αντικανονική χρήση:

Απαγορεύονται:

- Η χρήση του email για προσωπικούς σκοπούς, εμπορική δραστηριότητα ή παράνομες ενέργειες.
- Η χρήση του λογαριασμού email για έκφραση απόψεων «εκ μέρους της υπηρεσίας» χωρίς άδεια.
- Η χρήση ψευδών ή παραπλανητικών στοιχείων αποστολέα.
- Η δημιουργία καταπόνησης στους servers της υπηρεσίας (spamming, chain letters, μαζική αποστολή emails).

Υποχρεώσεις:

Οι χρήστες πρέπει:

- Να ελέγχουν το email τους καθημερινά.
- Να χρησιμοποιούν σαφή και περιεκτικό τίτλο στα μηνύματα.
- Να επαληθεύουν τη διεύθυνση παραλήπτη πριν την αποστολή.
- Να διαγράφουν παλιά μηνύματα (και από τον φάκελο «Διαγραμμένα»).
- Να αλλάζουν τους κωδικούς πρόσβασης τακτικά.
- Να αποφεύγουν ανοίγματα συνημμένων από άγνωστες πηγές (κίνδυνος phishing/malware).
- Να ενημερώνουν άμεσα το Τμήμα Πληροφορικής για ύποπτα emails.

3) Διαδίκτυο

Ο Φορέας παρέχει πρόσβαση στο διαδίκτυο **αποκλειστικά για υπηρεσιακούς σκοπούς**.

Ο Φορέας:

- διατηρεί το δικαίωμα περιορισμού πρόσβασης σε ιστοτόπους υψηλού κινδύνου,
- δύναται να επιβλέπει διαδικτυακές υπηρεσίες για λόγους ασφάλειας,
- δεν εγγυάται την ασφάλεια ή ακεραιότητα των πληροφοριών που λαμβάνονται από το διαδίκτυο,
- ενημερώνει ότι η υπεύθυνη χρήση μειώνει κινδύνους (ιούς, κακόβουλα λογισμικά, phishing).

Αντικανονική χρήση

Απαγορεύεται:

- Η πρόσβαση σε μέσα κοινωνικής δικτύωσης ή ιστότοπους άσχετους με τα καθήκοντα του Φορέα.

- Η αποστολή αρχείων μέσω διαδικτύου, **εκτός** πολύ μεγάλων αρχείων που δεν αποστέλλονται με e-mail και **μόνο** για υπηρεσιακούς λόγους.
- Η χρήση εργαλείων απομακρυσμένης πρόσβασης χωρίς έγκριση της Διοίκησης και του Τμήματος Πληροφορικής.
- Η πρόσβαση σε ιστοτόπους streaming (YouTube κ.ά.), εκτός αν απαιτείται για υπηρεσιακούς λόγους.
- Η χρήση του διαδικτύου που προκαλεί καταπόνηση ή κινδύνους ασφαλείας.
- Η χρήση ιστοτόπων μετατροπής αρχείων (pdf-to-word κ.λπ.), λόγω κινδύνου διαρροής δεδομένων.

Υποχρεώσεις

Οι χρήστες να:

- αλλάζουν συχνά κωδικούς πρόσβασης,
- μην αφήνουν κωδικούς εκτεθειμένους,
- ενημερώνουν άμεσα το Τμήμα Πληροφορικής για ύποπτη συμπεριφορά των συστημάτων,
- χρησιμοποιούν το διαδίκτυο μόνο όταν είναι απαραίτητο.

4) Διαχείριση και αποθήκευση έντυπων εγγράφων

Κανονική χρήση:

Οι υπάλληλοι οφείλουν να χειρίζονται και να αποθηκεύουν τα έντυπα έγγραφα με τρόπο που διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους. Συγκεκριμένα:

- Τα έγγραφα αποθηκεύονται σε **ασφαλείς, κλειδωμένες ντουλάπες ή ερμάρια**, στα οποία έχουν πρόσβαση μόνο τα εξουσιοδοτημένα άτομα του Φορέα.
- Οι ντουλάπες και τα γραφεία **κλειδώνονται** μετά το πέρας της εργασίας ή κάθε φορά που δεν παρίσταται στον χώρο εξουσιοδοτημένος υπάλληλος του Γραφείου / Τμήματος / Διεύθυνσης.
- Τα αρχεία πρέπει να **ταξινομούνται** με βάση την επίσημη δομή του Φορέα (π.χ. ημερομηνία, θέμα, υπηρεσία) και οι ντουλάπες να φέρουν **εξωτερική κωδικοποίηση** (π.χ. αριθμούς ή σύμβολα) ώστε να αποτρέπεται η αναγνώριση του περιεχομένου από μη εξουσιοδοτημένα άτομα.
- Για την αποφυγή άσκοπης συσσώρευσης εγγράφων, τηρείται **ένα μόνο φυσικό αρχείο** ανά υπόθεση ή διαδικασία, κατά προτίμηση στο σημείο πρωτογενούς διαχείρισης, αποφεύγοντας πολλαπλά αντίγραφα σε διαφορετικούς χώρους.
- Οι υπάλληλοι πρέπει να εφαρμόζουν τη **«συνήθεια καθαρού γραφείου»**, δηλαδή να μην αφήνουν έγγραφα εκτεθειμένα, ειδικά όταν περιέχουν

προσωπικά ή ευαίσθητα δεδομένα, είτε κατά τη διάρκεια σύντομης απουσίας είτε στο τέλος της ημέρας.

- Η αποστολή έντυπων εγγράφων γίνεται **υποχρεωτικά σε κλειστούς, σφραγισμένους φακέλους**, ώστε να μην είναι ορατό το περιεχόμενό τους.
- Η αποστολή εγγράφων μέσω τηλεομοιοτυπίας (fax) πραγματοποιείται μόνο αφού προηγηθεί **τηλεφωνική επιβεβαίωση** με τον παραλήπτη ώστε να διασφαλιστεί ότι βρίσκεται στο μηχάνημα κατά τη στιγμή λήψης του εγγράφου.

Αντικανονική χρήση:

Ως αντικανονική χρήση θεωρούνται όλες οι ενέργειες που μπορεί να θέσουν σε κίνδυνο τα έντυπα έγγραφα ή να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση.

Ενδεικτικά και όχι περιοριστικά:

- Η αποθήκευση υπηρεσιακών αρχείων σε χώρους προσβάσιμους από μη εξουσιοδοτημένους υπαλλήλους, εξωτερικούς συνεργάτες ή επισκέπτες.
- Η αποθήκευση αρχείων σε περιοχές με κινδύνους φυσικής καταστροφής, όπως υγρασία, θερμότητα, έκθεση σε νερό, κίνδυνο πυρκαγιάς ή άλλους περιβαλλοντικούς παράγοντες.
- Η αποθήκευση σε χώρους που δεν ασφαλίζουν ή παραμένουν ανεξέλεγκτοι κατά τη διάρκεια της ημέρας.
- Η μεταφορά υπηρεσιακών αρχείων σε τρίτους χώρους ή άτομα χωρίς έγκριση της υπηρεσίας.
- Η αποστολή εγγράφων με τηλεομοιότυπο (fax) χωρίς έγκριση ή χωρίς διαδικασία διασφάλισης παραλήπτη.
- Η μη εξουσιοδοτημένη καταστροφή εγγράφων ή η απόρριψή τους σε μη ασφαλή σημεία.
- Η παραποίηση υπηρεσιακών εγγράφων.
- Η φωτογράφιση ή βιντεοσκόπηση εγγράφων της υπηρεσίας με οποιαδήποτε συσκευή, συμπεριλαμβανομένων των προσωπικών κινητών τηλεφώνων.

Οι συντάξαντες

Στέφανος Τράικος

Κωνσταντίνος Οικονόμου

Πολύκαρπος Καρακατσάνης