PROSET
MANAGEMENT & CONSULTING

# ΔΗΜΟΣ ΚΙΛΚΙΣ

## Ρόλοι, Ευθύνες και Καθήκοντα GDPR

*(GDPR Roles, Responsibilities and Authorities)*

# ΔΗΜΟΣ ΚΙΛΚΙΣ

## Ρόλοι, Ευθύνες και Καθήκοντα GDPR

*(GDPR Roles, Responsibilities and Authorities)*

| | |
|---|---|
| **Κατάταξη Εγγράφου:** | **Εσωτερικό Έγγραφο** |
| **Έγγραφο Αναφ.** | **GDPR-DOC-05** |
| **Έκδοση:** | **1** |
| **Ημερομηνία:** | **29 Νοεμβρίου 2018** |

## Ιστορικό Αλλαγών

| Έκδοση | Ημερομηνία | Σύνοψη αλλαγών |
|---|---|---|
| | | |
| | | |

## Έγκριση

| Όνομα | Θέση | Υπογραφή | Ημερομηνία |
|---|---|---|---|
| | | | |

# Περιεχόμενα

# 1 Εισαγωγή

Ο «Δήμος Κιλκίς» χειρίζεται πολύ σοβαρά την ασφάλεια των προσωπικών του δεδομένων και τη συνεχή συμμόρφωση με τον GDPR. Ένα από τα βασικά χαρακτηριστικά μιας αποτελεσματικής προσέγγισης για την ασφάλεια των πληροφοριών είναι η σαφής κατανομή των ρόλων, κάθε ένας με καθορισμένες αρμοδιότητες και αρχές. Κάθε ένας από αυτούς τους ρόλους κατανέμεται σε συγκεκριμένα άτομα ή ομάδες εντός του «Δήμου Κιλκίς».

Είναι ζωτικής σημασίας ο καθένας εντός του Δήμου να κατανοεί το ρόλο που πρέπει να διαδραματίσει στη διαφύλαξη των πληροφοριών που διατηρούμε και επεξεργαζόμαστε σχετικά με τα άτομα. Αυτό το έγγραφο πρέπει να διαβάζεται σε συνδυασμό με άλλα που καθορίζουν τον τρόπο διαχείρισης της ασφάλειας των πληροφοριών μέσα στον «Δήμο Κιλκίς», συμπεριλαμβανομένων:

- *GDPR-DOC-17 Πολιτική Προστασίας Απορρήτου και Προσωπικών Δεδομένων*
- *GDPR-DOC-09 Διαδικασία Ανάπτυξης Ικανοτήτων GDPR*
- *GDPR-DOC-10 Πρόγραμμα Επικοινωνίας GDPR*
- *GDPR-DOC-15Διαδικασία Αντιμετώπισης Περιστατικών Ασφάλειας Πληροφοριών*
- *GDPR-DOC-18Διαδικασία Γνωστοποίησης Παραβιάσεων Προσωπικών Δεδομένων*
- *GDPR-DOC-22Διαδικασία Αιτήματος των Υποκειμένων των Δεδομένων*

Εξασφαλίζοντας ότι οι ρόλοι, οι αρμοδιότητες και τα καθήκοντα είναι σαφώς καθορισμένα, μπορούμε να αποτρέψουμε την εμφάνιση πολλών περιστατικών ασφάλειας πληροφοριών που αφορούν τα προσωπικά δεδομένα και να αντιδράσουμε αποτελεσματικά και κατάλληλα αν και όταν χρειάζεται.

# 2 Ρόλοι Ασφάλειας Πληροφοριών

Μέσα στο πλαίσιο της ασφάλειας των πληροφοριών που σχετίζεται με τη συμμόρφωσή μας με το GDPR, πρέπει να καθοριστούν και να διανεμηθούν οι ακόλουθοι κύριοι ρόλοι:

- Ομάδα Καθοδήγησης Ασφάλειας Πληροφοριών
- Διαχειριστής Ασφάλειας Πληροφοριών
- Ιδιοκτήτης Στοιχείων Πληροφοριών
- Υπεύθυνος Προστασίας Δεδομένων

Οι συγκεκριμένες ευθύνες και αρμοδιότητες καθενός από αυτούς τους ρόλους παρουσιάζονται σε επόμενα τμήματα του παρόντος εγγράφου.
Υπάρχουν επίσης ιδιαίτερες ευθύνες για την ασφάλεια των πληροφοριών που πρέπει να διεξάγονται από τους υφιστάμενους εσωτερικούς ρόλους εντός του Δήμου και αυτές παρουσιάζονται επίσης συνοπτικά μέσα σε αυτό το έγγραφο.

Αυτοί οι ρόλοι είναι:

- Τεχνικοί IT
- Χρήστες IT

Σε γενικές γραμμές, οι ευθύνες που ισχύουν για όλους τους εργαζομένους, τους εξωτερικούς συνεργάτες και άλλα ενδιαφερόμενα μέρη καθορίζονται στο πλαίσιο των σχετικών οργανωτικών πολιτικών. Ένα άτομο μπορεί να αναλαμβάνει περισσότερους του ενός ρόλους

# 3 Ειδικές Ευθύνες Ρόλου

Αυτή η ενότητα περιγράφει λεπτομερώς τις συγκεκριμένες ευθύνες και αρμοδιότητες ασφάλειας πληροφοριών για κάθε ρόλο στο πλαίσιο του «Δήμου Κιλκίς». Δεν περιλαμβάνει άλλους τύπους ευθύνης, πχ. τεχνικό και δεν πρέπει να θεωρείται ως πλήρης περιγραφή θέσης εργασίας. Οι ικανότητες που απαιτούνται για την εκπλήρωση κάθε ρόλου καθορίζονται στο έγγραφο GDPR-DOC-09 Διαδικασία Ανάπτυξης Ικανοτήτων GDPR.

## 3.1 Ομάδα Καθοδήγησης Ασφάλειας Πληροφοριών

Η Ομάδα Καθοδήγησης για την Ασφάλεια Πληροφοριών επιβλέπει τη συμμόρφωση με το GDPR και τη λειτουργία των ελέγχων ασφάλειας πληροφοριών ως εκπρόσωπος της ανώτατης διοίκησης στο «Δήμο Κιλκίς» και φέρει τη συνολική ευθύνη για την αποτελεσματικότητά του.

### *3.1.1 Μέλη*

Η ομάδα αποτελείται από μέλη της ανώτατης ομάδας διαχείρισης και περιλαμβάνει τουλάχιστον τους ακόλουθους ρόλους:

- Υπεύθυνος Προστασίας Προσωπικών Δεδομένων
- Διαχειριστής Ασφάλειας Πληροφοριών

Περαιτέρω μέλη μπορούν να διορίζονται από τα υπάρχοντα μέλη με βάση τις ανάγκες τους.

### *3.1.2 Ευθύνες*

Η Ομάδα Καθοδήγησης για την Ασφάλεια Πληροφοριών έχει τις ακόλουθες αρμοδιότητες:

- Διατήρηση μιας σαφούς και τρέχουσας κατανόησης της νομοθεσίας του GDPR και των συνεπειών της στις λειτουργικές διαδικασίες του Δήμου
- Καθιέρωση και διατήρηση της πολιτικής, των στόχων και των σχεδίων της ασφάλειας των πληροφοριών
- Επικοινωνία της σημασίας της συμμόρφωσης με το GDPR, την επίτευξη των στόχων και την ανάγκη συνεχούς βελτίωσης σε ολόκληρο το «Δήμο Κιλκίς»
- Συνειδητοποίηση των υπηρεσιακών αναγκών και των σημαντικών αλλαγών
- Διασφάλιση ότι οι απαιτήσεις ασφάλειας πληροφοριών καθορίζονται και πληρούνται με στόχο την ελαχιστοποίηση του κινδύνου και τη διατήρηση αποτελεσματικών ελέγχων για το «Δήμο Κιλκίς» και για τους πολίτες
- Προσδιορισμός και παροχή πόρων για το σχεδιασμό, την εφαρμογή, την παρακολούθηση, την αναθεώρηση και τη βελτίωση της ασφάλειας και της διαχείρισης των πληροφοριών, πχ. να προσλαμβάνει το κατάλληλο προσωπικό, να διαχειρίζεται το κύκλο εργασιών του προσωπικού
- Επιβλέπει τη διαχείριση των κινδύνων για το «Δήμο Κιλκίς»και τις υπηρεσίες του
- Διεξαγωγή ελέγχων διαχείρισης της ασφάλειας των πληροφοριών, σε προγραμματισμένα χρονικά διαστήματα, για να διασφαλιστεί η συνεχής καταλληλότητα, επάρκεια και αποτελεσματικότητα
- Επιλέγει ελεγκτές και εξασφαλίζει ότι οι εσωτερικοί έλεγχοι διενεργούνται με αντικειμενικό και αμερόληπτο τρόπο
- Καθιέρωση πολιτικής συνεχούς βελτίωσης όσον αφορά την ασφάλεια των πληροφοριών για το «Δήμο Κιλκίς»
- Ανασκόπηση σημαντικών περιστατικών ασφάλειας πληροφοριών
- Εξασφάλιση ότι οι ρυθμίσεις που αφορούν τους εξωτερικούς οργανισμούς που έχουν πρόσβαση σε συστήματα και υπηρεσίες πληροφοριών βασίζονται σε επίσημη συμφωνία που ορίζει όλες τις απαραίτητες απαιτήσεις ασφάλειας

- Σχεδιάζει, καταρτίζει, εφαρμόζει και διατηρεί ένα πρόγραμμα ελέγχου που περιλαμβάνει τη συχνότητα, τις μεθόδους, τις ευθύνες, τις απαιτήσεις σχεδιασμού και την αναφορά

#### *3.1.3 Καθήκοντα*

Η ομάδα καθοδήγησης για την ασφάλεια πληροφοριών έχει την εξουσία να:

- Εγκρίνει σημαντικές δαπάνες για ζητήματα που αφορούν την ασφάλεια των πληροφοριών
- Προσλαμβάνει πρόσθετους πόρους για τη διαχείριση της ασφάλειας των πληροφοριών
- Εγκρίνει πολιτικές υψηλού επιπέδου για την ασφάλεια των πληροφοριών
- Εκκινεί ενέργειες διαχείρισης περιστατικών υψηλού επιπέδου

### 3.2 Διαχειριστής Ασφάλειας Πληροφοριών

Ο Διαχειριστής Ασφάλειας Πληροφοριών είναι ένας τεχνικός ρόλος που εμπλέκεται στην υλοποίηση και τη συντήρηση πολλών από τους ελέγχους που χρησιμοποιούνται για τη διαχείριση του κινδύνου.

#### *3.2.1 Ευθύνες*

Ο Διαχειριστής Ασφάλειας Πληροφοριών έχει τις εξής ευθύνες:

- Υποβολή εκθέσεων στην Ομάδα Καθοδήγησης για την Ασφάλεια Πληροφοριών σε όλα τα θέματα που σχετίζονται με την ασφάλεια σε τακτική και ad hoc βάση, όταν απαιτείται
- Επικοινωνεί την πολιτική ασφάλειας των πληροφοριών σε όλα τα ενδιαφερόμενα μέρη, όπου ενδείκνυται, συμπεριλαμβανομένων των πελατών
- Εφαρμογή των απαιτήσεων της πολιτικής ασφάλειας πληροφοριών
- Διαχείριση κινδύνων που σχετίζονται με την πρόσβαση στην υπηρεσία ή τα συστήματα
- Βεβαίωση ότι έχουν τεθεί σε λειτουργία και τεκμηριωθούν οι έλεγχοι ασφαλείας
- Διαχειρίζεται την καθημερινή συντήρηση των ελέγχων, όπως:
    - Έλεγχος πρόσβασης (κύκλος ζωής λογαριασμού χρήστη)
    - Δοκιμή και εφαρμογή των ενημερωμένων εκδόσεων ασφαλείας
    - Σάρωση ευπάθειας
    - Λειτουργία λογισμικού ασφάλειας πχ. IDS, IPS, τείχη προστασίας, DLP
    - Ασφάλιση συστήματος και δικτύου
    - Απομακρυσμένη πρόσβαση

- Διαχείριση κρυπτογραφικού κλειδιού
- Διαχείριση αρχείων καταγραφής

- Προσδιορισμός και διαχείριση περιστατικών ασφάλειας πληροφοριών σύμφωνα με μια διαδικασία

#### *3.2.2 Καθήκοντα*

Ο Διαχειριστής Ασφάλειας Πληροφοριών έχει την εξουσία:

- Να λάβει μέτρα για να αποτρέψει την εμφάνιση ή την κλιμάκωση περιστατικού ασφάλειας των πληροφοριών, όπου είναι δυνατόν
- Να διατηρήσει τα αρχεία ασφαλείας πληροφοριών σύμφωνα με τις καθορισμένες πολιτικές και διαδικασίες
- Δηλώνει περιστατικά ασφάλειας πληροφοριών
- Ελέγχει τη λειτουργία των ελέγχων σε όλους τους τομείς δραστηριότητας

### 3.3 Ιδιοκτήτης Στοιχείων Πληροφοριών

Ο Ιδιοκτήτης Στοιχείων Πληροφοριών έχει πρωταρχική επιχειρησιακή ευθύνη για ένα ή περισσότερα πληροφοριακά στοιχεία όπως ορίζονται στο έγγραφο *GDPR-DOC-13 Απογραφή Στοιχείων Προσωπικών Δεδομένων* που υποδεικνύει πού αποθηκεύονται τα προσωπικά δεδομένα.

#### *3.3.1 Ευθύνες*

Ο Ιδιοκτήτης Στοιχείων Πληροφοριών έχει τις ακόλουθες ευθύνες:

- Είναι υπεύθυνος για συγκεκριμένα στοιχεία πληροφοριών
- Διατηρεί και επανεξετάζει τους ελέγχους ασφαλείας για τα κατανεμημένα στοιχεία ενεργητικού
- Συμμετέχει σε αξιολογήσεις κινδύνου σχετικά με τα στοιχεία του
- Βεβαιώνει ότι η σχετική εγγραφή στο απόθεμα στοιχείων είναι ενημερωμένη

#### *3.3.2 Καθήκοντα*

Ο Ιδιοκτήτης Στοιχείων Πληροφοριών έχει την εξουσία να:

- Εφαρμόζει ελέγχους σε σχέση με τα στοιχεία πληροφοριών που βρίσκονται υπό τον έλεγχό τους

## 3.4 Υπεύθυνος Προστασίας Δεδομένων

Ο Υπεύθυνος Προστασίας Δεδομένων παρέχει τις υπηρεσίες του για την ορθή λειτουργία του οργανισμού σε θέματα προστασίας Προσωπικών Δεδομένων.

### *3.4.1 Ευθύνες*

Ο Υπεύθυνος Προστασίας Δεδομένων έχει τις ακόλουθες ευθύνες:

- Ενημερώνει και συμβουλεύει το «Δήμο Κιλκίς» και τους υπαλλήλους που δεσμεύονται να εκτελούν την επεξεργασία βάσει της ισχύουσας νομοθεσίας περί προστασίας δεδομένων
- Παρακολουθεί τη συμμόρφωση με τον GDPR και με τις πολιτικές του «Δήμου Κιλκίς» σε σχέση με την προστασία των προσωπικών δεδομένων
- Να επικαιροποιεί τις διαδικασίες και τις πολιτικές που εφαρμόζονται από το «Δήμο Κιλκίς» για την συμμόρφωσή της με τον GDPR
- Ενημερώνει και καταρτίζει το προσωπικό που ασχολείται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και τους σχετικούς ελέγχους ασφάλειας
- Παρέχει συμβουλές, όταν ζητούνται, σχετικά με εκτιμήσεις αντίκτυπου προστασίας δεδομένων και παρακολούθηση της απόδοσής τους

### *3.4.2 Καθήκοντα*

Ο Υπεύθυνος Προστασίας Δεδομένων έχει το καθήκον να:

- Συμβουλεύει το «Δήμο Κιλκίς» σχετικά με τις αιτήσεις υποκειμένων δεδομένων που επιτρέπονται βάσει της σχετικής νομοθεσίας για την προστασία των δεδομένων

# 4 Άλλοι Ρόλοι με Ευθύνες Ασφάλειας Πληροφοριών

Υπάρχουν διάφοροι άλλοι εσωτερικοί ρόλοι μέσα στο Δήμο, οι οποίοι, αν και δεν είναι αποκλειστικά αφιερωμένοι στην ασφάλεια των πληροφοριών, έχουν σχετικές αρμοδιότητες και αρχές.

## 4.1 Τεχνικοί IT

Λόγω του συχνά τεχνικού χαρακτήρα των ζητημάτων ασφάλειας των πληροφοριών, οι τεχνικοί IT έχουν να διαδραματίσουν σημαντικό ρόλο στην παροχή και συντήρηση των ελέγχων.

### *4.1.1 Ευθύνες*

Οι Τεχνικοί IT έχουν γενικά τις ακόλουθες ευθύνες:

- Λειτουργία διαδικασιών όπως διαχείριση συμβάντων και αλλαγών
- Παροχή τεχνικής εμπειρογνωμοσύνης σε θέματα ασφάλειας των πληροφοριών
- Εφαρμογή τεχνικών ελέγχων
- Διαχείριση συστήματος πχ. δημιουργία χρηστών, δημιουργία αντιγράφων ασφαλείας
- Παρακολούθηση ασφαλείας πχ. δικτυακές εισβολές

### *4.1.2 Καθήκοντα*

Ένας Τεχνικός IT έχει την εξουσία να:

- Να λάβει μέτρα για να αποτρέψει την εμφάνιση ή την κλιμάκωση περιστατικού ασφάλειας των πληροφοριών, όπου είναι δυνατόν μετά από ενημέρωση και έγκριση του Διαχειριστή Ασφάλειας Πληροφοριών

## 4.2 Χρήστες IT

Οι ευθύνες των χρηστών IT ορίζονται σε μια ποικιλία πολιτικών σε όλη την οργάνωση και συνοψίζονται εν συντομία μόνο παρακάτω.

### *4.2.1 Ευθύνες*

Ένας χρήστης IT έχει τις ακόλουθες κύριες αρμοδιότητες:

- Να βεβαιωθεί ότι γνωρίζει και συμμορφώνεται με όλες τις πολιτικές ασφάλειας του Δήμου που σχετίζονται με τον επιχειρησιακό του ρόλο
- Να αναφέρει τυχόν πραγματικές ή πιθανές παραβιάσεις ασφαλείας
- Να συμβάλλει στην εκτίμηση επικινδυνότητας όπου απαιτείται

### *4.2.2 Καθήκοντα*

Ένας χρήστης IT έχει την εξουσία να:

- Λάβει μέτρα για να αποτρέψει την εμφάνιση ή την κλιμάκωση περιστατικού ασφάλειας των πληροφοριών, όπου είναι δυνατόν μετά από ενημέρωση και έγκριση του Διαχειριστή Ασφάλειας Πληροφοριών