



# ΔΗΜΟΣ ΚΙΛΚΙΣ

**Διαδικασία GDPR  
Αξιολόγησης Προμηθευτή  
(*Supplier GDPR  
Assessment Procedure*)**



# ΔΗΜΟΣΚΙΛΚΙΣ

## Διαδικασία GDPR Αξιολόγησης Προμηθευτή (*Supplier GDPR Assessment Procedure*)

<b>Ταξινόμηση Εγγράφου:</b>	<b>Εσωτερικό έγγραφο</b>
<b>Έγγραφο Ανάφ.</b>	<b>GDPR-DOC-23</b>
<b>Έκδοση:</b>	<b>1</b>
<b>Χρονολογημένο:</b>	<b>29 Νοεμβρίου 2018</b>
<b>Συντάκτης Εγγράφου:</b>	<b>Proset I.K.E</b>

### Ιστορικό Αλλαγών

Έκδοση	Ημερομηνία	Συντάκτης Αναθεώρησης	Σύνοψη Αλλαγών

### Έγκριση

Όνομα	Θέση	Υπογραφή	Ημερομηνία

## Περιεχόμενα

1	Εισαγωγή.....	4
2	<b>Διαδικασία GDPR Αξιολόγησης Προμηθευτή.....</b>	<b>4</b>
2.1	Προϋποθέσεις.....	4
2.2	Χρονοδιάγραμμα και Προγραμματισμός.....	4
2.3	Διαδικασία.....	5
2.4	Χειρισμός Σφαλμάτων.....	6
2.5	Υποστήριξη και Κλιμάκωση.....	6
2.6	Έλεγχος και Καταγραφή.....	6
2.7	Παρακολούθηση.....	6

## Κατάλογος Πινάκων

<i>ΠΙΝΑΚΑΣ 1 – ΔΙΑΧΕΙΡΙΣΗ ΣΦΑΛΜΑΤΩΝ.....</i>	<i>6</i>
<i>Πίνακας 2 – Πληροφορίες Επικοινωνίας για Υποστήριξη.....</i>	<i>6</i>

## 1 Εισαγωγή

Η χρήση κατάλληλων, ασφαλών και αποτελεσματικών προμηθευτών είναι καθοριστικής σημασίας για τη συμμόρφωση του «Δήμου Κιλκίς» με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Οι προμηθευτές χρησιμοποιούνται όχι μόνο για να βοηθήσουν στη λειτουργία μιας αποτελεσματικής παροχής υπηρεσίας αλλά σε πολλές περιπτώσεις για την παροχή υπηρεσιών απευθείας στον πολίτη, όπως στην περίπτωση της φιλοξενίας ιστοσελίδων.

Άλλοι, παίζουν καθοριστικό ρόλο στο κατά πόσο ο «Δήμος Κιλκίς» επιτυγχάνει την επίτευξη των στόχων της, για παράδειγμα στην προσέλκυση επαρκών επισκεπτών στην ιστοσελίδα της.

Όμως, οι προμηθευτές όχι μόνο πρέπει να προσφέρουν σωστά και ποιοτικά προϊόντα και υπηρεσίες, αλλά πρέπει να το κάνουν και με ασφαλή τρόπο, ο οποίος δεν θέτει σε κίνδυνο τον «Δήμο Κιλκίς» και τα προσωπικά δεδομένα των πελατών της. Αυτή η διαδικασία έχει σκοπό να εξασφαλίσει ότι λαμβάνονται επαρκή μέτρα και να διερευνηθεί κατά πόσο ένας προμηθευτής ανταποκρίνεται στις υποχρεώσεις του GDPR

Τα ακόλουθα έγγραφα σχετίζονται με τη διαδικασία αυτή:

- *GDPR-DOC-17 Πολιτική Προστασίας Απορρήτου και Προσωπικών Δεδομένων*
- *GDPR-FORM-14 Αξιολόγηση Προμηθευτή GDPR*

## 2 Διαδικασία GDPR Αξιολόγησης Προμηθευτή

### 2.1 Προϋποθέσεις

Πριν ξεκινήσετε τη διαδικασία, θα πρέπει να ισχύουν οι ακόλουθες προϋποθέσεις:

- Έχουν καθοριστεί απαιτήσεις για ένα προϊόν ή μια υπηρεσία
- Ο προμηθευτής θα (ή ήδη) αποθηκεύει και επεξεργάζεται τα προσωπικά δεδομένα των πελατών, των εργαζομένων ή άλλων ενδιαφερομένων

### 2.2 Χρονοδιάγραμμα και Προγραμματισμός

Αυτή η διαδικασία μπορεί να ξεκινήσει καθ όλη την διάρκεια του έργου, όμως είναι ορθό να συμβαδίζει χρονικά με την χαρτογράφηση των προσωπικών δεδομένων.

## 2.3 Διαδικασία

Για την αξιολόγηση του προμηθευτή (Απαιτήσεις GDPR) θα πρέπει να συμπληρώνεται η φόρμα Αξιολόγησης Προμηθευτή **GDPR-FORM-14 Αξιολόγηση Προμηθευτή GDPR**. Οι συμπληρωμένες φόρμες θα πρέπει να αποθηκεύονται στον φάκελο του συστήματος διαχείρισης προσωπικών δεδομένων, ως τεκμηρίωση της αξιολόγησης

Απαιτούνται τα ακόλουθα βήματα:

1. Χρησιμοποιήστε ένα νέο αντίγραφο της φόρμας **GDPR-FORM-14 Αξιολόγηση Προμηθευτή GDPR** και καταγράψτε τα στοιχεία της αξιολόγησης, συμπεριλαμβανομένης της ημερομηνίας/ώρας, του ονόματος του αξιολογητή, της εταιρείας που αξιολογείται, του ονόματος του προϊόντος ή της υπηρεσίας και της ταξινόμησης των προσωπικών δεδομένων που είναι ή μπορούν να μοιραστούν με προμηθευτές.
2. Διερευνήστε τα στοιχεία της εταιρείας που παρέχει το προϊόν ή την υπηρεσία, συμπεριλαμβανομένου του καταχωρημένου ονόματος, της χώρας εγγραφής, του κατά προσέγγιση μεγέθους και το χρόνο σύστασης.
3. Τεκμηριώστε τα εμπορικά στοιχεία της υπό εξέταση προσφοράς, συμπεριλαμβανομένων των συμβατικών όρων, συμπεριλαμβανομένου του μήκους, του εφαρμοστέου δικαίου, της αναθεώρησης και της λήξης.
4. Ανακαλύψτε ποιες πληροφορίες είναι διαθέσιμες σχετικά με τους ελέγχους ασφάλειας πληροφοριών που χρησιμοποιεί ο προμηθευτής, συμπεριλαμβανομένων των πολιτικών ασφάλειας πληροφοριών, πιστοποιήσεις (πχ. ISO / IEC 27001, Cyber-Essentials), κρυπτογράφηση κλπ.
5. Καθορίστε ποια προσωπικά δεδομένα διατηρούνται ή υποβάλλονται σε επεξεργασία από τον προμηθευτή και για ποιο λόγο. Αυτό θα πρέπει να περιλαμβάνει βαθμίδες και εάν υπάρχουν ειδικές κατηγορίες.
6. Καθορίστε τη φυσική θέση των προσωπικών δεδομένων, δηλ. τη χώρα ή τις χώρες στις οποίες βρίσκεται ο εξοπλισμός(hardware) στον οποίο βρίσκονται τα δεδομένα. Για λόγους GDPR, αυτό θα γίνει εντός της Ευρωπαϊκής Ένωσης ή σε μια χώρα της οποίας το πλαίσιο προστασίας δεδομένων θεωρήθηκε αποδεκτό από την ΕΕ.
7. Καταγράψτε τι ελέγχους εφαρμόζει ο προμηθευτής για την προστασία των προσωπικών δεδομένων, όπως η κρυπτογράφηση σε κατάσταση ηρεμίας και ο έλεγχος πρόσβασης.
8. Βεβαιωθείτε αν ο προμηθευτής χρησιμοποιεί τρίτους για την παροχή της υπηρεσίας και εάν αυτοί θα έχουν πρόσβαση στα προσωπικά δεδομένα. Αν ναι, αυτή η διαδικασία πρέπει να επαναληφθεί για κάθε τρίτο.

9. Όταν έχουν ληφθεί και καταγραφεί όλες οι σχετικές πληροφορίες, αξιολογήστε κατά πόσον πρέπει να ληφθούν περαιτέρω μέτρα για να εξασφαλιστεί η συμμόρφωση με το GDPR. Καταγράψτε αυτές τις ενέργειες στη φόρμα και να διασφαλίσετε ότι αυτές γνωστοποιούνται και ξεκινάει η εφαρμογή τους.

## 2.4 Χειρισμός Σφαλμάτων

Στα πλαίσια αυτής της διαδικασίας ενδέχεται να παρουσιαστούν τα ακόλουθα συνήθη σφάλματα:

Στάδιο Επεξεργασίας	Σφάλμα	Πιθανή Αιτία	Συνιστώμενη Ενέργεια

Πίνακας1–Διαχείριση Σφαλμάτων

## 2.5 Υποστήριξη και Κλιμάκωση

Εάν παρουσιαστεί σφάλμα το οποίο δεν μπορεί να διορθωθεί χρησιμοποιώντας αυτή τη διαδικασία, θα πρέπει να λάβετε υποστήριξη χρησιμοποιώντας τις ακόλουθες πληροφορίες:

Πρόσωπο Υποστήριξης	Ρόλος	Email	Ώρες Διαθεσιμότητας

Πίνακας2–Πληροφορίες Επικοινωνίας για Υποστήριξη

## 2.6 Έλεγχος και Καταγραφή

Οι αξιολογήσεις GDPR των προμηθευτών και τα αποτελέσματά τους, καταγράφονται στη φόρμα *GDPR-FORM-14 Αξιολόγηση Προμηθευτή GDPR* και αποθηκεύονται στη δομή του φακέλου του συστήματος διαχείρισης.

## 2.7 Παρακολούθηση

Η πρόοδος των αξιολογήσεων θα πρέπει να παρακολουθείται τουλάχιστον εβδομαδιαίως.