

Δήμος Κιλκίς

Πρόγραμμα Επικοινωνίας GDPR

GDPR Communication Program



Δήμος Κιλκίς

Πρόγραμμα Επικοινωνίας GDPR

GDPR Communication Program

Ταξινόμηση Εγγράφου:

Εσωτερικό Έγγραφο

Έγγραφο Ανάφ.	GDPR-DOC-10
Έκδοση:	1
Χρονολογημένο:	29 Νοεμβρίου 2018
Συντάκτης Εγγράφου:	Proset I.K.E

Ιστορικό Αλλαγών

Έκδοση	Ημερομηνία	Σύνοψη αλλαγών

Έγκριση

Όνομα	Θέση	Υπογραφή	Ημερομηνία

Περιεχόμενα

1 Εισαγωγή.....	4
2 Πρόγραμμα Επικοινωνίας.....	5
2.1 Κοινό.....	5
2.2 Θέματα Επικοινωνίας.....	5
2.3 Μέθοδοι Επικοινωνίας.....	6
2.4 Ανατροφοδότηση σχετικά με την Επικοινωνία.....	8
3 Συμπέρασμα.....	8

Κατάλογος Πινάκων

<i>Πίνακας 1 – Μέθοδοι Επικοινωνίας.....</i>	<i>7</i>
<i>Πίνακας 2 – Κάτοχοι Σχέσεων.....</i>	<i>8</i>

1 Εισαγωγή

Ο GDPR, έχει νομική ισχύ από τον Μάιο του 2018 και επεκτείνει και διευκρινίζει τα δικαιώματα των υποκειμένων των δεδομένων και τους τρόπους με τους οποίους πρέπει να ενεργούν οι οργανισμοί που διατηρούν και επεξεργάζονται τα προσωπικά δεδομένα των πολιτών της ΕΕ. Ως μέρος του ευρωπαϊκού δικαίου, η συμμόρφωση με το GDPR δεν είναι προαιρετική και ο «Δήμος Κιλκίς» δεσμεύεται πλήρως να διασφαλίσει ότι πληροί όλες τις απαιτήσεις του.

Στα πλαίσια των 173 αιτιολογικών σκέψεων και 99 άρθρων, το GDPR περιέχει κάποιες σημαντικές αλλαγές σε σχέση με τον προηγούμενο νόμο για την προστασία των δεδομένων, ο οποίος ποίκιλε μεταξύ των διαφόρων κρατών της ΕΕ. Στις εν λόγω αλλαγές συμπεριλαμβάνονται η υποχρεωτική γνωστοποίηση της παραβίασης δεδομένων, πρόστιμα έως και 4% του συνολικού παγκόσμιου κύκλου εργασιών, ο διορισμός ενός υπεύθυνου προστασίας δεδομένων και η χρήση εκτιμήσεων αντικτύπου σχετικά με την προστασία δεδομένων.

Υπάρχει έντονη ανάγκη να γνωστοποιηθούν αυτές οι αλλαγές, οι επιπτώσεις τους και η προσέγγισή μας για την αντιμετώπιση αυτών στα ενδιαφερόμενα μέρη, όπως είναι οι εργαζόμενοι, οι πελάτες, οι εργολάβοι, οι μέτοχοι και οι προμηθευτές, ώστε όλοι να γνωρίζουν τι συμβαίνει όσον αφορά το GDPR.

Το παρόν έγγραφο καθορίζει τον τρόπο με τον οποίο η Ομάδα Καθοδήγησης Ασφάλειας Πληροφοριών (GDPR-DOC-05 Ρόλοι Ευθύνες και Καθήκοντα GDPR) θα ενημερώνει τα ενδιαφερόμενα μέρη, τόσο εντός όσο και εκτός του «Δήμου Κιλκίς», σχετικά με το θέμα του GDPR και τους ελέγχους ασφάλειας πληροφοριών που χρησιμοποιούμε για να υπάρχει συνεχής συμμόρφωση. Προσδιορίζει ποια είναι τα ενδιαφερόμενα μέρη και πώς θα δημιουργηθεί ένα αποτελεσματικό κανάλι επικοινωνίας.

2 Πρόγραμμα Επικοινωνίας

Η γενική προσέγγιση που θα ακολουθήσει η Ομάδα Καθοδήγησης Ασφάλειας Πληροφοριών για την εξασφάλιση αποτελεσματικής δέσμευσης και επικοινωνίας σε σχέση με το GDPR εντός του «Δήμου Κιλκίς» έχει ως εξής:

1. Θα πρέπει να προσδιορίζεται πάντα στην αρχή το κοινό / ενδιαφερόμενα μέρη
2. Θα καθορίζονται τα θέματα επικοινωνίας για κάθε ενδιαφερόμενο μέρος
3. Θα συμφωνούνται οι καταλληλότερες μεθόδους δέσμευσης και επικοινωνίας
4. Θα γίνεται εφαρμογή του προγράμματος
5. Θα υπάρχει ανταπόκριση σε κάθε ανατροφοδότηση και θα υπάρχουν καταγραφές ώστε σε ύστερο στάδιο και για λόγους συνεχούς βελτίωσης να ανασκοπείται η επιτυχία της επικοινωνίας.

Αυτά τα βήματα εξετάζονται ξεχωριστά στις ακόλουθες ενότητες.

2.1 Κοινό

Το παρόν πρόγραμμα επικοινωνίας απευθύνεται στα ενδιαφερόμενα μέρη, εσωτερικά και εξωτερικά, συμβεβλημένα και μόνιμα, τα οποία έχουν ένα ρόλο να διαδραματίσουν στην προστασία των προσωπικών δεδομένων στο «Δήμο Κιλκίς».

Τα ενδιαφερόμενα μέρη περιλαμβάνουν:

- Διοικητικό συμβούλιο/Διευθύνων Σύμβουλος/Πρόεδρος
- Προμηθευτές
- Πολίτες
- Εποπτική Αρχή Προστασίας Δεδομένων
- Υπάλληλοι του Δήμου
- Εξωτερικοί συνεργάτες που παρέχουν υπηρεσίες στο Δήμο
- Ευρύ κοινό
- Μέσα Μαζικής Ενημέρωσης

2.2 Θέματα Επικοινωνίας

Το πρόγραμμα επικοινωνίας αποσκοπεί στην ενημέρωση των βασικών στοιχείων των πληροφοριών στους ακόλουθους κύριους τομείς:

- Οι βασικές απαιτήσεις του GDPR και του τρόπου με τον οποίο σχετίζονται με την επεξεργασία των προσωπικών δεδομένων από τον «Δήμο Κιλκίς»
- Το γενικό πλαίσιο που χρησιμοποιήθηκε για την εκπλήρωση των απαιτήσεων του GDPR, συμπεριλαμβανομένου του οράματος, των πολιτικών, των σχεδίων και των στόχων που πρέπει να επιτευχθούν
- Το ρόλο που αναμένεται να διαδραματίσει κάθε ενδιαφερόμενο μέρος για την εξασφάλιση της συμμόρφωσης
- Νέες και τροποποιημένες επεξεργασίες και διαδικασίες που εφαρμόζονται ή πρόκειται να τεθούν σε εφαρμογή

- Πώς τα ισχύοντα μέτρα ασφάλειας των πληροφοριών αφορούν την εκπλήρωση του GDPR, τόσο τώρα όσο και στη συνέχεια
- Οποιοσδήποτε άλλες κανονιστικές, ρυθμιστικές και συμβατικές υποχρεώσεις και περιορισμοί εντός των οποίων πρέπει να λειτουργεί ο «Δήμος Κιλκίς» σε σχέση με τα προσωπικά δεδομένα
- Ενημερώσεις σχετικά με τον τρόπο με τον οποίο τα σχέδια προχωρούν προς την κατεύθυνση της επίτευξης των καθορισμένων στόχων του πλαισίου συμμόρφωσης με το GDPR
- Ενημέρωση για τα ζητήματα και τους κινδύνους της ασφάλειας πληροφοριών και της προσέγγισής μας στην αντιμετώπισή τους

Το επίπεδο λεπτομέρειας που απαιτείται στους προαναφερθέντες τομείς ποικίλλει μεταξύ των ενδιαφερομένων μερών.

2.3 Μέθοδοι Επικοινωνίας

Υπάρχουν ορισμένες καθιερωμένες μέθοδοι επικοινωνίας εντός του Δήμου και αυτές θα χρησιμοποιηθούν όπου είναι δυνατόν. Αυτές περιλαμβάνουν:

Μέθοδος	Περιγραφή
Ενημέρωση Διοίκησης	Προφορική ή και έντυπη ενημέρωση σύντομης αναφοράς
Ενημερωτικά δελτία	Αποστολή με e-mail ενημέρωσης για σημαντικά γεγονότα που σχετίζονται με το GDPR
Ηλεκτρονικά μηνύματα	Επείγουσα ενημέρωση με γεγονότα κυρίως ασφάλειας για άμεση αντίδραση
Συναντήσεις προμηθευτών υποστήριξης	Η Ομάδα Καθοδήγησης Ασφάλειας Πληροφοριών ή ο Διαχειριστής Ασφάλειας Πληροφοριών εξετάζουν με κάθε προμηθευτή τα θέματα αλλαγών ή αναβαθμίσεων σε υπηρεσίες που έχουν επιπτώσεις στον GDPR
Ενημέρωση μέσω ιστοτόπου	Όλες οι δημόσιες ανακοινώσεις για θέματα GDPR που μπορούν να αφορούν τους εμπλεκόμενους με το Δήμο (Πολίτες, Υπαλλήλους)
Ενημέρωση Πολιτών	Προφορική ή και έντυπη ενημέρωση κατά την επίσκεψή τους στους χώρους του Δήμου
Εκπαίδευση	Η εκπαίδευση του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων, καθώς και σε ειδικές σχετικές με ασφάλεια λειτουργίες του πληροφοριακού συστήματος

Όπου ενδείκνυται, θα θεσπιστούν πρόσθετες μέθοδοι, είτε προσωρινά είτε μόνιμα, για να συμπληρωθούν οι ήδη διαθέσιμες.

Η κατανομή των τρόπων με τους οποίους οι αναγκαίες πληροφορίες θα κοινοποιηθούν στα ενδιαφερόμενα μέρη παρουσιάζεται στον πίνακα 1.

Ενδιαφερόμενο Μέρος	Αντικείμενο Επικοινωνίας	Μέθοδος(οι)	Συχνότητα
Εκτελεστική Διοίκηση	Απαιτήσεις GDPR Στρατηγική ασφάλειας πληροφοριών, Διαχείριση κινδύνου υψηλού επιπέδου, Ρύθμιση πολιτικής Αναφορές υψηλού επιπέδου	Ενημέρωση Διοίκησης	Εξαμηνιαία
Χρήστες IT	Ενημέρωση για την πολιτική ασφάλειας πληροφοριών, Ad-hoc υπενθυμίσεις όταν εμφανίζονται σημαντικά γεγονότα πχ. παραβιάσεις, Προειδοποιήσεις και ευαισθητοποίηση.	Ενημερωτικά δελτία, Ηλεκτρονικά μηνύματα, Ενημέρωση μέσω ιστοτόπου,	Εξαμηνιαία
Χρήστες IT	Η εκπαίδευση του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων, καθώς και σε ειδικές σχετικές με την ασφάλεια του πληροφοριακού συστήματος	Εκπαίδευση	Ετήσια και κατά την πρόσληψη
Προμηθευτές υποστήριξης	Πολιτική ασφάλειας πληροφοριών , Συμβατικές απαιτήσεις, Υποχρεώσεις προμηθευτών, Προτάσεις για βελτίωση	Συνεδριάσεις με προμηθευτές	Εξαμηνιαία
Πολίτες	Δικαιώματα των υποκειμένων των δεδομένων και διαδικασίες υποβολής αιτήσεων, Πολιτική απορρήτου, Επιτόπιοι έλεγχοι	Ενημέρωση μέσω ιστοτόπου, Ενημέρωση Πολιτών	Συνεχής

Πίνακας1–Μέθοδοι Επικοινωνίας

2.4 Ανατροφοδότηση σχετικά με την Επικοινωνία

Για κάθε ενδιαφερόμενο μέρος, καθορίζεται ένας αρμόδιος, ο οποίος θα είναι υπεύθυνος για τη λήψη σχολίων σχετικά με την επιτυχία της επικοινωνίας και τη διαχείριση της σε συνεχή βάση. Οι αρμόδιοι εμφανίζονται στον παρακάτω πίνακα.

Ενδιαφερόμενο Μέρος	Κάτοχος Σχέσης
Εκτελεστική Διοίκηση	Υπεύθυνος Ασφάλειας Πληροφοριών
Χρήστες IT	Υπεύθυνος Ασφάλειας Πληροφοριών

Πολίτες	Υπεύθυνος Ασφάλειας Πληροφοριών
---------	---------------------------------

Πίνακας2–Κάτοχοι Σχέσεων

Ανασκοπήσεις θα γίνονται με κάθε ενδιαφερόμενο τουλάχιστον μία φορά το χρόνο. Μπορούν να πραγματοποιούνται και συχνότερα εάν η ανώτατη διεύθυνση θεωρεί ότι δικαιολογείται.

Οι παρατηρήσεις σχετικά με την επιτυχία της επικοινωνίας θα συγκεντρωθούν, θα αξιολογηθούν από την Ομάδα Καθοδήγησης Ασφάλειας Πληροφοριών και, κατά περίπτωση, θα ενσωματωθούν στο πρόγραμμα το συντομότερο δυνατόν.

3 Συμπέρασμα

Η επίτευξη αποτελεσματικής επικοινωνίας με τα ενδιαφερόμενα μέρη είναι απολύτως καθοριστική για τη διασφάλιση της συμμόρφωσης με το GDPR στο πλαίσιο του «Δήμου Κιλκίς». Οι μέθοδοι επικοινωνίας που αναφέρονται στο παρόν έγγραφο εξασφαλίζουν ότι όλοι οι ενδιαφερόμενοι παραμένουν καλά ενημερωμένοι σχετικά με τα θέματα προστασίας δεδομένων και ασφάλειας των πληροφοριών και έχουν την ευκαιρία να παρέχουν ανατροφοδότηση τόσο για τα χρησιμοποιούμενα κανάλια επικοινωνίας όσο και για το περιεχόμενό τους.