PROSET
MANAGEMENT & CONSULTING

Δήμος Κιλκίς

Διαδικασία
Ανάπτυξης Ικανοτήτων GDPR

GDPR Competence
Development Procedure

Δήμος Κιλκίς

Διαδικασία
Ανάπτυξης Ικανοτήτων GDPR

GDPR Competence
Development Procedure

Ταξινόμηση Εγγράφου:	**Εσωτερικό Έγγραφο**
Έγγραφο Ανάφ.	**GDPR-DOC-09**
Έκδοση:	1
Χρονολογημένο:	**29 Νοεμβρίου 2018**
Συντάκτης Εγγράφου:	**Proset I.K.E**

Ιστορικό Αλλαγών

Έκδοση	Ημερομηνία	Σύνοψη αλλαγών

Έγκριση

Όνομα	Θέση	Υπογραφή	Ημερομηνία

Περιεχόμενα

Κατάλογος Πινάκων

1 Εισαγωγή

Προκειμένου να προστατευθούν τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται, αποθηκεύονται και υποβάλλονται σε επεξεργασία από το Δήμο, είναι απαραίτητο οι εργαζόμενοι και τα άλλα ενδιαφερόμενα μέρη που εμπλέκονται στην παροχή αποτελεσματικής ασφάλειας πληροφοριών να έχουν τις απαιτούμενες ικανότητες. Οι συνέπειες της έλλειψης επαρκών δεξιοτήτων μπορεί να οδηγήσουν σε προβλήματα πόρων, μη συμμόρφωσης με τις νομικές απαιτήσεις και αυξημένο κίνδυνο για τον Δήμο πχ. στην εισαγωγή των ιών.

Ο «Δήμος Κιλκίς» δίνει έμφαση στην παροχή κατάρτισης για την κάλυψη των αναγκών του Δήμου και την ανάπτυξη υπαλλήλων ώστε να μπορούν να εκπληρώσουν καλύτερα τους ρόλους τους. Για την τεχνολογία πληροφοριών (IT) πρέπει να διασφαλιστεί ότι αναπτύσσονται και διατηρούνται συγκεκριμένες τεχνολογικές δεξιότητες μέσα στο Δήμο, ιδίως καθώς αυτές μπορούν να αλλάξουν γρήγορα καθώς αναπτύσσεται η τεχνολογία, για παράδειγμα με νέες εκδόσεις λογισμικού ή με την εισαγωγή νέων συστημάτων και ελέγχων.

Σκοπός αυτής της διαδικασίας ανάπτυξης ικανοτήτων είναι να προσδιοριστεί εάν υπάρχουν επαρκείς ικανότητες σχετικά με την ασφάλεια των πληροφοριών στους ανάλογους τομείς του «Δήμου Κιλκίς» και ποιες δεξιότητες μπορεί να απαιτούνται στο εγγύς μέλλον για να αντιμετωπιστούν οι γνωστές αλλαγές που επηρεάζουν το «Δήμο Κιλκίς».

Για να γίνει αυτό, πρέπει να προσδιοριστούν τα απαιτούμενα επίπεδα αρμοδιοτήτων για κάθε ρόλο GDPR και ασφάλειας πληροφοριών και, στη συνέχεια, να συγκριθούν με την κατανόηση των υφιστάμενων επιπέδων αρμοδιότητας εκείνων που εκπληρώνουν τους ρόλους τους για να παράσχουν συστάσεις για περαιτέρω ανάπτυξη ικανοτήτων.

Η διαδικασία αυτή πρέπει να συνδυαστεί με τα ακόλουθα έγγραφα που παρέχουν περισσότερες λεπτομέρειες σχετικά με το πλαίσιο, το πεδίο εφαρμογής, τους στόχους, τους πόρους και τους ρόλους, τις αρμοδιότητες και τις αρχές που σχετίζονται με τη συμμόρφωση με το GDPR:

- *GDPR-DOC-17 Πολιτική Προστασίας Απορρήτου και Προσωπικών Δεδομένων*
- *GDPR-DOC-05 Ρόλοι Ευθύνες και Καθήκοντα GDPR*
- *GDPR-DOC-15 Διαδικασία Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών*

2 Διαδικασία Ανάπτυξης Ικανοτήτων

Τα βήματα για την ανάπτυξη των κατάλληλων ικανοτήτων περιγράφονται σε αυτό το κεφάλαιο.

2.1 Αξιολόγηση Απαιτήσεων ως προς τις Αρμοδιότητες ανά Ρόλο

Οι διάφοροι ρόλοι και τα καθήκοντα που απαιτούνται για τη διαχείριση και τη βελτίωση της συμμόρφωσης με τον GDPR περιγράφονται στο έγγραφο *GDPR-DOC-05 Ρόλοι, Ευθύνες και Εξουσίες GDPR* και αυτοί διατίθενται σε ένα ή περισσότερα συγκεκριμένα άτομα εντός του «Δήμου Κιλκίς». Σε πολλές περιπτώσεις, ένας καθορισμένος ρόλος αποτελεί μέρος ενός ευρύτερου, γενικότερου ρόλου που εκπληρώνει το άτομο, δηλαδή ο χρόνος του ατόμου δεν είναι αποκλειστικά αφιερωμένος στην ασφάλεια των πληροφοριών.

Ακολουθούν οι ακόλουθοι ρόλοι που σχετίζονται με τη GDPR και την ασφάλεια πληροφοριών:

- Ομάδα Καθοδήγησης για την Ασφάλεια Πληροφοριών
- Διαχειριστής της Ασφάλειας Πληροφοριών
- Κάτοχος Πληροφοριακών Στοιχείων
- Υπεύθυνος Προστασίας Δεδομένων

Προκειμένου να εκπληρώσει τις ευθύνες ενός ρόλου, ένα άτομο πρέπει να διαθέτει ορισμένες βασικές ικανότητες σε ένα κατάλληλο επίπεδο. Το **Παράρτημα Α** αυτής της διαδικασίας δίνει ένα αρχικό σημείο εκκίνησης για τον κατάλογο των βασικών αρμοδιοτήτων που απαιτούνται από κάθε ρόλο. Ο κατάλογος αυτός πρέπει να ενημερώνεται κάθε φορά που χρησιμοποιείται αυτή η διαδικασία για να αντικατοπτρίζει αλλαγές στις αρμοδιότητες που απαιτούνται λόγω τεχνολογικής, οργανωτικής ή άλλης αιτίας. Συνιστάται να γίνει αυτό σε στενή συνεργασία με τους διευθυντές και τα ίδια τα άτομα, έτσι ώστε να συμπεριληφθούν όλες οι σχετικές αρμοδιότητες.

Εκτός από τον προσδιορισμό των ίδιων των αρμοδιοτήτων, πρέπει να επιτευχθεί συμφωνία για το επίπεδο των απαιτούμενων αρμοδιοτήτων. Αυτό πρέπει να γίνει με αναφορά στους ορισμούς των επιπέδων αρμοδιοτήτων που παρουσιάζονται στον **Πίνακα 1** παρακάτω.

Θα πρέπει να ληφθούν υπόψη οι υφιστάμενες και γνωστές μελλοντικές απαιτήσεις για τη συμμόρφωση με το GDPR πχ. εάν ένα συγκεκριμένο εργαλείο λογισμικού βρίσκεται σε διαδικασία υλοποίησης, η αρμοδιότητα γι' αυτό πρέπει να συμπεριληφθεί στον αντίστοιχο κατάλογο υπό τον κατάλληλο ρόλο.

Το αποτέλεσμα αυτού του βήματος της διαδικασίας είναι ένας κατάλογος ρόλων με τις απαιτούμενες αρμοδιότητες και επίπεδα αρμοδιοτήτων.

2.2 Αξιολόγηση των Υφιστάμενων Επιπέδων Ικανότητας

Προκειμένου να εκτιμηθούν τα τρέχοντα επίπεδα ικανοτήτων των ατόμων που πρόκειται να εκπληρώσουν συγκεκριμένους ρόλους, νομοθετικούς και σχετικούς με την ασφάλεια πληροφοριών, χρησιμοποιείται μια προσέγγιση ερωτηματολογίου. Πρώτα, προσδιορίζονται οι άνθρωποι που πρόκειται να αναλάβουν κάθε ρόλο.

Στη συνέχεια δημιουργείται ένα κατάλληλο ερωτηματολόγιο για κάθε ρόλο που περιλαμβάνει όλες τις αρμοδιότητες που έχουν προσδιοριστεί ως απαιτούμενες για τον ρόλο αυτό. Τα απαιτούμενα επίπεδα αρμοδιοτήτων δεν πρέπει να περιλαμβάνονται στο ερωτηματολόγιο. Όλοι οι αρμόδιοι υπάλληλοι καλούνται στη συνέχεια να συμπληρώσουν το ερωτηματολόγιο όσο το δυνατόν αντικειμενικά χρησιμοποιώντας τους ορισμούς των επιπέδων αρμοδιοτήτων που αναφέρονται στον παρακάτω πίνακα.

Επίπεδο Ικανότητας	Σύνοψη	Οδηγίες
0	Κανένα	Δεν έχετε καμία γνώση ή εμπειρία σε αυτόν τον τομέα και δεν είναι μέρος του ρόλου σας.
1	Χαμηλό	Ο τομέας αρμοδιοτήτων χρησιμοποιείται σπάνια και βασίζεται σε μεγάλο βαθμό στην παρατήρηση του τρόπου με τον οποίο το κάνουν οι άλλοι, με ελάχιστη κατανόηση του γιατί εκτελούνται συγκεκριμένα καθήκοντα. Ίσως ο τομέας αρμοδιότητας να ασκείται μόνο για σχετικά σύντομο χρονικό διάστημα και δεν θεωρείται μέρος του ρόλου εργασίας του ατόμου. Δεν δόθηκε καμία επίσημη εκπαίδευση. Μια γενική ευαισθητοποίηση.
2	Μέτριο	Ο τομέας αρμοδιοτήτων ασκείται τακτικά ως μέρος του ρόλου της εργασίας και αυτό πιθανότατα συμβαίνει για μια αρκετά μεγάλη περίοδο ώστε το άτομο να αισθάνεται άνετα να το κάνει (περισσότερο από ένα χρόνο). Μπορεί να έχει ληφθεί άτυπη και σε ορισμένες περιπτώσεις επίσημη εκπαίδευση και υπάρχει κατανόηση των αρχών που διέπουν την ικανότητα. Το άτομο αισθάνεται ικανό σε αυτόν τον τομέα.
3	Υψηλό	Ο τομέας αρμοδιοτήτων θεωρείται ως μια ιδιαίτερη δύναμη και υποστηρίζεται από σημαντική κατάρτιση, προσόντα και εμπειρία για μεγάλο χρονικό διάστημα (πιθανώς περισσότερο από 3 χρόνια). Οι αρχές είναι πλήρως κατανοητές και το άτομο ενημερώνεται για τις εξελίξεις στον τομέα αυτό. Μπορεί να έχουν εκπαιδεύσει άλλους και να είναι υπεύθυνοι για την ανάπτυξη διαδικασιών και να έχουν συμμετάσχει σε πολλά έργα που να έχουν χρησιμοποιήσει την ικανότητά τους.

Επίπεδο Ικανότητας	Σύνοψη	Οδηγίες
4	Άριστο	Το άτομο αναγνωρίζεται εξωτερικά ως εμπειρογνώμονας, ο οποίος συμβάλλει στις εξελίξεις σε αυτόν τον τομέα και μπορεί να συμμετέχει σε εκδηλώσεις του τομέα όπως η παρουσίαση σε συνέδρια και σεμινάρια. Αυτός / αυτή αποπνέει μεγάλη εκτίμηση στους προμηθευτές και τους πελάτες και μπορεί να βοηθήσει στην ανάπτυξη και δοκιμή νέων προϊόντων και υπηρεσιών.

Πίνακας 1 – Ορισμοί επιπέδων ικανότητας

Οι απαντήσεις των ατόμων πρέπει στη συνέχεια να επικυρωθούν από άλλο μέρος, ανάλογα με τη φύση του ρόλου του ατόμου. Αυτός μπορεί να είναι ο διευθυντής ή ο επιβλέπων του ατόμου ή, σε κατάλληλες περιπτώσεις, μπορεί να χρησιμοποιηθεί μια μέθοδος αξιολόγησης από ομότιμους. Αυτό θα πρέπει να διασφαλίζει ένα αυξημένο επίπεδο συνέπειας στις απαντήσεις, καθώς κάποιοι άνθρωποι είναι πιο πιθανό να υπερεκτιμήσουν ή να υποτιμήσουν τα επίπεδα ικανοτήτων τους σε σχέση με άλλα. Όταν υπάρχει διαφωνία σχετικά με ένα επίπεδο αρμοδιότητας, η κατάσταση πρέπει να συζητηθεί με το σχετικό άτομο για να κατανοηθεί ο λόγος της απόκλισης. Εάν υπάρχει διαρκής διαφωνία, πρέπει να ληφθεί απόφαση από τη διοίκηση σχετικά με το ποιο επίπεδο θα πρέπει να χρησιμοποιηθεί.

2.3 Καθορισμός Ενεργειών Ανάπτυξης Ικανοτήτων

Αφού έχει καθοριστεί μια σαφής εικόνα των απαιτούμενων και των υφιστάμενων δεξιοτήτων για ένα άτομο μέσα σε ένα ρόλο, οι διαφορές μπορούν να αναθεωρηθούν προκειμένου να προσδιοριστεί η ανάγκη για ενέργειες ανάπτυξης. Αυτό μπορεί να γίνει χρησιμοποιώντας μια μέθοδο όπως φαίνεται στον Πίνακα 2 παρακάτω.

Στις προτεινόμενες ενέργειες ανάπτυξης, μπορεί να εξεταστούν μία ή περισσότερες από τις ακόλουθες εναλλακτικές λύσεις:

- Ανεπίσημη εκπαίδευση από υπάρχον προσωπικό με υψηλότερο επίπεδο αρμοδιοτήτων, πχ. καθοδήγηση
- Επίσημη εκπαίδευση μέσω ηλεκτρονικών μαθημάτων ή μαθημάτων στην τάξη
- Πρόσληψη πρόσθετου προσωπικού με τις σχετικές αρμοδιότητες
- Χρήση πόρων τρίτων μερών σε ad-hoc βάση, πχ. εργολάβους ή συμβούλους
- Χρήση πόρων τρίτων μέσω συμφωνητικού συμπεφωνημένης υποστήριξης που παρέχει εγγυημένη πρόσβαση στο απαιτούμενο επίπεδο επάρκειας

Η επιλογή της προσέγγισης μπορεί να εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένων των διαθέσιμων εσωτερικών πόρων, του προϋπολογισμού και των χρονοδιαγραμμάτων.

Σε ορισμένες περιπτώσεις, μπορεί να αποφασιστεί να μην αναληφθεί δράση για την αντιμετώπιση ενός αντιληπτού ελλείμματος στην αρμοδιότητα, πχ. εάν η απαίτηση

είναι πιθανό να μειωθεί ή να εξαφανιστεί στο εγγύς μέλλον λόγω γνωστών αλλαγών. Οι κίνδυνοι που συνδέονται με αυτό πρέπει να δηλώνονται με σαφήνεια.

Οι δράσεις ανάπτυξης και οι κίνδυνοι που συνιστώνται για αποδοχή στη συνέχεια υποβάλλονται στη διοίκηση για έγκριση.

Όνομα:
Ρόλος:

Αρμοδιότητα	Απαιτούμενο Επίπεδο	Πραγματικό Επίπεδο	Διαφορά	Προτεινόμενη Ενέργεια Ανάπτυξης	Προτεραιότητα

Πίνακας 2 – Προσδιορισμός των ενεργειών ανάπτυξης

2.4 Αξιολόγηση της Αποτελεσματικότητας

Οι εγκεκριμένες ενέργειες που εντοπίστηκαν για την ανάπτυξη ικανοτήτων σε συγκεκριμένα άτομα θα πρέπει να επανεξεταστούν για αποτελεσματικότητα τόσο στο πλαίσιο των αναθεωρήσεων των επιδόσεων των εργαζομένων όσο και στις τακτικές αξιολογήσεις της διοίκησης για τη συμμόρφωση με το GDPR

Μόλις ολοκληρωθεί μια ενέργεια ανάπτυξης, θα πρέπει να πραγματοποιηθεί επαναξιολόγηση για να εξακριβωθεί ότι έχει οδηγήσει στο άτομο να διαθέτει το απαιτούμενο επίπεδο επάρκειας. Σε αντίθετη περίπτωση, θα πρέπει να καθοριστούν οι λόγοι για αυτό και, αν χρειαστεί, να προσδιοριστούν περαιτέρω δράσεις για την επίτευξη του απαιτούμενου αποτελέσματος.

Θα πρέπει να διατηρηθούν τα κατάλληλα τεκμηριωμένα στοιχεία για όλες τις ενέργειες που διεξάγονται. Αυτό μπορεί να περιλαμβάνει τα αρχεία κατάρτισης, τα ημερολόγια καθοδήγησης ή τις συμβάσεις τρίτων.

3 Παράρτημα Α: Απαιτούμενες Αρμοδιότητες ανά Ρόλο

Οι ακόλουθοι κατάλογοι προορίζονται να λειτουργήσουν ως αφετηρία για τις ικανότητες που απαιτούνται για κάθε έναν από τους ρόλους που σχετίζονται με τη συμμόρφωση με το GDPR.

3.1 Ομάδα Καθοδήγησης για την Ασφάλεια Πληροφοριών

Αρμοδιότητα	Απαιτούμενο Επίπεδο
Νομοθεσία GDPR, ερμηνεία και νομολογία	3
Έννοια, σχεδιασμός και έλεγχος της Ασφάλειας Πληροφοριών	3
Σχεδιασμός, θέσπιση, εφαρμογή και διατήρηση ενός προγράμματος ελέγχου	3
Διαχείριση κινδύνου της Ασφάλειας Πληροφοριών	3
Πολιτικές της Ασφάλειας Πληροφοριών	3
Διεξαγωγή ανασκοπήσεων της διοίκησης	3
Αρχές ελέγχου	2
Συνεχής βελτίωση	2
Διαχείριση περιστατικών της Ασφάλειας Πληροφοριών	2

3.2 Διαχειριστής της Ασφάλειας Πληροφοριών

Αρμοδιότητα	Απαιτούμενο Επίπεδο
Έννοιες της ασφάλειας πληροφοριών	2
Διαχείριση περιστατικών της ασφάλειας πληροφοριών	2
Αρχές των ελέγχων της ασφαλείας πληροφοριών	2
Διαχείριση κινητών συσκευών	3
Ταξινόμηση πληροφοριών	3
Διαχείριση μέσων ενημέρωσης	3
Διαχείριση πρόσβασης χρηστών	3

Αρμοδιότητα	Απαιτούμενο Επίπεδο
Διαχείριση κρυπτογραφικού κλειδιού	3
Αντίγραφα ασφαλείας των πληροφοριών	3
Έννοιες της ασφάλειας πληροφοριών	3
Διαχείριση περιστατικών της ασφάλειας πληροφοριών	3
Αρχές των ελέγχων της ασφαλείας πληροφοριών	3
Διαχείριση κινητών συσκευών	3

3.3 Κάτοχος Πληροφοριακών Στοιχείων

Αρμοδιότητα	Απαιτούμενο Επίπεδο
Έννοιες, σχεδιασμός και έλεγχος της ασφάλειας πληροφοριών	2
Διαχείριση κινδύνου της ασφάλειας πληροφοριών	3
Εκτιμήσεις αντικτύπου σχετικά με την προστασία δεδομένων	2
Διαχείριση στοιχείων	3
Αρχές των ελέγχων της ασφαλείας πληροφοριών	2

3.4 Υπεύθυνος Προστασίας Δεδομένων

Αρμοδιότητα	Απαιτούμενο Επίπεδο
Νομοθεσία GDPR, ερμηνεία και νομολογία	3
Έννοιες, σχεδιασμός και έλεγχος της ασφάλειας πληροφοριών	2
Προστασία δεδομένων και σχετική νομοθεσία	3
Εκτιμήσεις αντικτύπου σχετικά με την προστασία δεδομένων	3
Διαχείριση κινδύνου της ασφάλειας πληροφοριών	3
Αρχές των ελέγχων της ασφαλείας πληροφοριών	3