ΔΗΜΟΣ ΚΙΛΚΙΣ

Οργανωτικά και τεχνικά μέτρα προστασίας

ΔΗΜΟΣ ΚΙΛΚΙΣ

Οργανωτικά και τεχνικά μέτρα προστασίας

Ταξινόμηση εγγράφων:	**Εσωτερικό έγγραφο**
Έγγραφο Αναφ.	**GDPR-DOC-01**
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

2 Μέτρα ασφαλείας

Μετά την αξιολόγηση του επιπέδου κινδύνου, ο **Δήμος Κιλκίς** πρέπει να προχωρήσει στη υλοποίηση ή την βελτίωση των οργανωτικών και τεχνικών μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων, σύμφωνα με τις προτάσεις της **PROSET**.

Το παρόν κείμενο περιλαμβάνει τις προτάσεις της **PROSET** για συμμόρφωση και ενέργειες που θα πρέπει να αναλάβει η διοίκηση και το τεχνικό προσωπικό του **Δήμου Κιλκίς**.

Το έγγραφο αυτό διαβάζεται μαζί με τα:

- *GDPR-DOC-02 Παρουσίαση ενημέρωσης GDPR*
- *GDPR-DOC-12 Εκπαίδευση Ευαισθητοποίησης για την Ασφάλεια Πληροφοριών*
- *GDPR-DOC-05 Ρόλοι Ευθύνες και Καθήκοντα GDPR*
- *GDPR-DOC-17 Πολιτική Προστασίας Απορρήτου και Προσωπικών Δεδομένων*
- *GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων*
- *GDPR-DOC-15 Διαδικασία Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών*
- *GDPR-DOC-32 Σύνοψη Πολιτικής Αποδεκτής Χρήσης*

3 Οργανωτικά μέτρα ασφάλειας

3.1 Διαχείριση Ασφάλειας

3.1.1 Πολιτικές ασφάλειας και μεθοδολογίες για τη προστασία των προσωπικών δεδομένων

Η πολιτική ασφαλείας ***GDPR-DOC-17 Πολιτική Προστασίας Απορρήτου και Προσωπικών Δεδομένων*** είναι ένα έγγραφο υψηλού επιπέδου που θέτει τις βασικές αρχές για την ασφάλεια και την προστασία των προσωπικών δεδομένων σε έναν Δήμο. Έτσι, αποτελεί τη βάση για την εφαρμογή όλων των ειδικών τεχνικών και οργανωτικών μέτρων, σύμφωνα με το άρθρο. 32, όπως επίσης συμπληρώνεται από το άρθρο. 24 (εφαρμογή πολιτικών προστασίας δεδομένων).

Με βάση την πολιτική ασφάλειας, τα συγκεκριμένα τεχνικά και οργανωτικά μέτρα περιγράφονται σε ένα σύνολο λεπτομερέστερων πολιτικών / διαδικασιών (πχ. σχετικά με τον έλεγχο πρόσβασης, τη διαχείριση συσκευών, τη διαχείριση πόρων κλπ.).

Η πολιτική ασφάλειας δείχνει τη συνολική δέσμευση της διοίκησης του δήμου για ασφάλεια και προστασία δεδομένων. Μπορεί να βασίζεται ή να αποτελεί μέρος της γενικής πολιτικής ασφάλειας του οργανισμού στον τομέα της πληροφορικής και σε κάθε περίπτωση θα πρέπει να εξετάσει ρητά επίσης την προστασία των προσωπικών δεδομένων.

2.1.1.1	Η **PROSET** προτείνει την πολιτική όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως μέρος της πολιτικής ασφάλειας των πληροφοριών στο έγγραφο ***GDPR-DOC-17 Πολιτική Προστασίας Απορρήτου και Προσωπικών Δεδομένων***
2.1.1.2	Η πολιτική πρέπει να εγκριθεί από τη διοίκηση και να κοινοποιηθεί σε όλους τους υπαλλήλους και τους εξωτερικούς συνεργάτες
2.1.1.3	Η πολιτική ασφαλείας αναφέρεται: στους ρόλους και τις ευθύνες του προσωπικού, στα βασικά τεχνικά και οργανωτικά μέτρα που έχουν θεσπιστεί για την ασφάλεια των προσωπικών δεδομένων, στους φορείς επεξεργασίας δεδομένων ή σε άλλα τρίτα μέρη που εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα.
2.1.1.4	Η πολιτική προστασίας απορρήτου και προσωπικών δεδομένων θα πρέπει να επανεξετάζεται και να αναθεωρείται, εάν είναι απαραίτητο, ανά εξάμηνο.
	RelatedtoISO27001:2013- A.5Securitypolicy

3.1.2 Ρόλοι και ευθύνες

Σύμφωνα με άρθρο 32.4 «Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους ».

Επομένως, ως πρώτος και βασικός έλεγχος για την ασφάλεια των προσωπικών δεδομένων, όλες οι θέσεις του **Δήμου Κιλκίς** με πρόσβαση σε προσωπικά δεδομένα θα πρέπει να έχουν σαφώς καθορισμένες και τεκμηριωμένες ευθύνες, ρόλους και ανάγκη να γνωρίζουν τα βασικά (οι οποίες επανεξετάζονται και βελτιώνονται τακτικά).

Ένας ιδιαίτερα σημαντικός ρόλος είναι ο Διαχειριστής Ασφαλείας Πληροφοριών, ο οποίος είναι υπεύθυνος για την παρακολούθηση της ορθής εφαρμογής της πολιτικής ασφάλειας. Ένας άλλος σημαντικός ρόλος είναι ο Υπεύθυνος Προστασίας Δεδομένων (DPO), ο οποίος παρακολουθεί τη συμμόρφωση με το

GDPR και συνεπώς, είναι σαφές ότι πρέπει επίσης να συνεργαστεί με τον Διαχειριστή Ασφαλείας Πληροφοριών για την κατάλληλη εφαρμογή μέτρων ασφαλείας.

Ο Υπεύθυνος Προστασίας Δεδομένων (DPO)παρέχει τις υπηρεσίες του ως σύμβουλος καλύπτοντας τις ευθύνες του Υπεύθυνου Προστασίας Δεδομένων.

2.1.2.1	Η **PROSET** προτείνει τους ρόλους και τις ευθύνες που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο έγγραφο **GDPR-DOC-05 Ρόλοι Ευθύνες και Καθήκοντα GDPR** που καθορίζονται σαφώς και αναλύονται σύμφωνα με την πολιτική ασφάλειας.
2.1.2.1	Η Διοίκηση πρέπει να διορίσει επίσημα (τεκμηριωμένα) τον Διαχειριστή Ασφαλείας Πληροφοριών και τον Υπεύθυνο Προστασίας Δεδομένων (DPO). Τα καθήκοντα και οι ευθύνες τους καθορίζονται στο παραπάνω έγγραφο.
	RelatedtoISO27001:2013- A.6.1.1Informationsecurity rolesandresponsibilities

3.1.3 Πολιτική ελέγχου πρόσβασης

Η πολιτική ελέγχου πρόσβασης στα συστήματα που χρησιμοποιούνται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα περιγράφεται στο έγγραφο ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων***. Αυτό βασίζεται στην αρχή της «ανάγκης να γνωρίζει»,δηλαδή κάθε ρόλος / χρήστης θα πρέπει να έχει μόνο το επίπεδο πρόσβασης στα προσωπικά δεδομένα που είναι απολύτως απαραίτητο για την εκτέλεση των σχετικών καθηκόντων του. Αυτή είναι μια κεντρική ιδέα και στον GDPR και συνδέεται στενά με την αρχή της ελαχιστοποίησης των δεδομένων (άρθρο 5 (γ)).

Η πολιτική ελέγχου πρόσβασης θα εφαρμοστεί με μεταγενέστερα τεχνικά μέτρα, όπως περιγράφεται στο κεφάλαιο 4. Σημαντικό ρόλο στην υλοποίηση της πολιτικής έχει ο κάθε Προμηθευτής λογισμικού/Πληροφοριακών Συστημάτων.

2.1.3.1	Η **PROSET** προτείνει την πολιτική ελέγχου πρόσβασης, τόσο για τους εσωτερικούς χρήστες όσο και για τους εξωτερικούς συνεργάτες με απομακρυσμένη πρόσβαση, στο έγγραφο ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων*** το οποίο πρέπει να εγκρίνει η Διοίκηση
2.1.3.2	Ειδικά δικαιώματα ελέγχου πρόσβασης θα πρέπει να διατίθενται σε κάθε ρόλο (που εμπλέκεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα) σύμφωνα με την αρχή της ανάγκης γνώσης.
2.1.3.3	Οι ρόλοι με υπερβολικά δικαιώματα πρόσβασης θα πρέπει να ορίζονται σαφώς και να εκχωρούνται σε περιορισμένα ειδικά μέλη του προσωπικού.
	Related to ISO 27001:2013 - A.9.1.1 Access control policy

3.1.4 Διαχείριση πόρων/υποδομών

Η σωστή διαχείριση του υλικού, του λογισμικού και των πόρων του δικτύου είναι ουσιώδης για την ασφάλεια των προσωπικών δεδομένων, καθώς επιτρέπει τον έλεγχο των μέσων επεξεργασίας (και συνεπώς τον έλεγχο των επακόλουθων οργανωτικών και τεχνικών μέτρων). Η διαχείριση των πόρων περιλαμβάνει τουλάχιστον την εγγραφή πόρων πληροφορικής και τοπολογίας δικτύου (οι οποίοι χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων).

2.1.4.1	Ο **Δήμος Κιλκίς** πρέπει να διαθέτει μητρώο των πόρων πληροφορικής που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων (υλικό, λογισμικό και δίκτυο). Για το μητρώο θα χρησιμοποιηθεί το έγγραφο ***GDPR-FORM-15 Μητρώο Πόρων Πληροφορικής***
2.1.4.2	Οι πόροι πληροφορικής πρέπει να επανεξετάζονται και να ενημερώνονται σε ετήσια βάση.
2.1.4.3	Οι ρόλοι που έχουν πρόσβαση σε ορισμένους πόρους θα πρέπει να καθοριστούν και να τεκμηριωθούν.
	Related to ISO 27001:2013 - A.8 Asset management

3.1.5 Διαχείριση αλλαγών

Η διαχείριση των αλλαγών στοχεύει στον συγχρονισμό και τον έλεγχο όλων των αλλαγών που πραγματοποιούνται στο σύστημα πληροφορικής που χρησιμοποιείται για την επεξεργασία των προσωπικών δεδομένων. Πρόκειται για ένα σημαντικό μέτρο ασφάλειας, καθώς μια ανεπιτυχής προσπάθεια αλλαγής θα μπορούσε να οδηγήσει σε μη εξουσιοδοτημένη αποκάλυψη, τροποποίηση ή καταστροφή δεδομένων.

2.1.5.1	Η**PROSET** προτείνει μια πολιτική αλλαγών στο έγγραφο ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων*** το οποίο πρέπει να εγκρίνει η Διοίκηση. Ο **Δήμος Κιλκίς** θα πρέπει να διασφαλίζει ότι όλες οι αλλαγές στο σύστημα ΤΠ καταχωρούνται και παρακολουθούνται από ένα συγκεκριμένο άτομο (πχ. IT ή διαχειριστή ασφαλείας). Θα πρέπει να πραγματοποιείται τακτική παρακολούθηση αυτής της διαδικασίας.
	Related to ISO 27001:2013 - A. 12.1 Operational procedures and responsibilities

3.1.6 Ο εκτελών την επεξεργασία

Σύμφωνα με το άρθρο 28.1, «ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων». Το ίδιο άρθρο ορίζει ότι η επεξεργασία από τον εκτελούντα την επεξεργασία θα πρέπει κατ' ανάγκη να διέπεται από σύμβαση ή άλλη νομική πράξη, καθορίζοντας επίσης τις ελάχιστες ρήτρες που πρέπει να περιλαμβάνει και ειδικότερα την ασφάλεια των προσωπικών δεδομένων σύμφωνα με το άρθρο 32

2.1.6.1	Η **PROSET** προτείνει στο ***GDPR-DOC-17 Πολιτική Προστασίας Απορρήτου και Προσωπικών Δεδομένων*** τις ελάχιστες κατευθυντήριες γραμμές και διαδικασίες που καλύπτουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τους υπευθύνους επεξεργασίας δεδομένων (ανάδοχοι / εξωτερικοί συνεργάτες) που θα πρέπει να οριστούν, τεκμηριωθούν και συμφωνηθούν μεταξύ του **Δήμου Κιλκίς** και του εκτελούντος την επεξεργασία πριν από την έναρξη των δραστηριοτήτων επεξεργασίας. Αυτές οι κατευθυντήριες γραμμές και οι διαδικασίες θα πρέπει υποχρεωτικά να καθορίζουν το ίδιο επίπεδο ασφάλειας των προσωπικών δεδομένων που απαιτείται από την πολιτική ασφαλείας του οργανισμού.
2.1.6.2	Μόλις διαπιστώσει παραβίαση δεδομένων προσωπικού χαρακτήρα, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση.
2.1.6.3	Οι επίσημες απαιτήσεις και υποχρεώσεις πρέπει να συμφωνηθούν επισήμως μεταξύ του υπεύθυνου επεξεργασίας δεδομένων και του εκτελούντος την επεξεργασία. Ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να παρέχει επαρκή τεκμηριωμένα αποδεικτικά στοιχεία συμμόρφωσης. Εάν τα μέτρα προστασίας δεν θεωρηθούν επαρκή, τότε προτείνεται η διακοπή της συνεργασίας
2.1.6.4	Ο **Δήμος Κιλκίς** θα πρέπει να ελέγχει τακτικά τη συμμόρφωση του εκτελούντος την επεξεργασία με το συμφωνημένο επίπεδο απαιτήσεων και υποχρεώσεων.
2.1.6.5	Οι υπάλληλοι του επεξεργαστή δεδομένων που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα πρέπει να υπόκεινται σε συγκεκριμένες τεκμηριωμένες συμφωνίες εμπιστευτικότητας / μη δημοσιοποίησης πληροφοριών.
	Related to ISO 27001:2013 - A.15 Supplier relationships

3.2 Αντιμετώπιση περιστατικών και υπηρεσιακή συνέχεια

3.2.1 Διαχείριση παραβιάσεων προσωπικών δεδομένων

Είναι υποχρέωση από τον GDPR τα περιστατικά που επηρεάζουν δεδομένα προσωπικού χαρακτήρα και ενδέχεται να θέσουν σε κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων να αναφέρονται χωρίς αδικαιολόγητη καθυστέρηση στην εποπτική αρχή προστασίας δεδομένων, και όπου είναι εφικτό, εντός 72 ωρών από τη στιγμή που της επίγνωσης της παραβίασης. Σε περίπτωση που δεν επιτευχθεί ο στόχος των 72 ωρών, πρέπει να δοθούν λόγοι για την καθυστέρηση. Η διαχείριση των παραβιάσεων προσωπικών δεδομένων είναι μέρος της διαδικασίας αντιμετώπισης των παραβιάσεων ασφάλειας των πληροφοριών που περιγράφεται στη παράγραφο 2.2.2 στη συνέχεια

2.2.1.1	Διαχείριση περιστατικών παραβιάσεων προσωπικών δεδομένων περιγράφεται αναλυτικά στο έγγραφο ***GDPR-DOC-18 Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων*** το οποίο πρέπει να εγκρίνει η Διοίκηση.
2.2.1.2	Οι παραβιάσεις προσωπικών δεδομένων θα πρέπει να αναφέρονται άμεσα στη διεύθυνση. Πρέπει να εφαρμόζονται διαδικασίες γνωστοποίησης για την αναφορά των παραβιάσεων στις αρμόδιες αρχές και τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, σύμφωνα με το άρθρο. 33 και 34.
2.2.1.3	Τα περιστατικά και οι παραβιάσεις των προσωπικών δεδομένων θα πρέπει να καταγράφονται μαζί με λεπτομέρειες σχετικά με το συμβάν και τις μετέπειτα ενέργειες μετριασμού που εκτελούνται.
	Related to ISO 27001:2013 - A.16 Information security incident management

3.2.2 Υπηρεσιακή συνέχεια του οργανισμού

Ένα σχέδιο επιχειρησιακής (υπηρεσιακής) συνέχειας (Business Continuity Plan - BCP) είναι ουσιαστικής σημασίας για τον προσδιορισμό των διαδικασιών και των τεχνικών μέτρων που πρέπει να ακολουθήσει ο **Δήμος Κιλκίς** σε περίπτωση παραβίασης περιστατικών / προσωπικών δεδομένων(ασφάλεια εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας). Ως εκ τούτου, συμπληρώνει την πολιτική ασφαλείας του οργανισμού, καθώς και το σχέδιο απόκρισης επίπτωσης. Το μέτρο αυτό συνδέεται σαφώς με το άρθρο 32, το οποίο αναθέτει την ικανότητα (για τον υπεύθυνο επεξεργασίας / εκτελών την επεξεργασία) «να αποκαταστήσει εγκαίρως τη διαθεσιμότητα και την πρόσβαση σε προσωπικά δεδομένα σε περίπτωση φυσικού ή τεχνικού συμβάντος».

2.2.2.1	Το έγγραφο ***GDPR-DOC-15 Διαδικασία Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών*** είναι ένα σχέδιο αντιμετώπισης όποιου είδους περιστατικού που επηρεάζει την ασφάλεια των πληροφοριών και συνεπώς την λειτουργία του **Δήμου Κιλκίς**, συμπεριλαμβανομένων εκείνων που ενδεχομένως επηρεάζουν τα προσωπικά δεδομένα για τα οποία ο οργανισμός είναι υπεύθυνος.
2.2.2.2	Το ***GDPR-DOC-15 Διαδικασία Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών*** είναι λεπτομερές και τεκμηριωμένο (σύμφωνα με τη γενική πολιτική ασφαλείας). Περιλαμβάνει σαφείς ενέργειες και ανάθεση ρόλων.
2.2.2.3	Ένα επίπεδο εγγυημένης ποιότητας των υπηρεσιών θα πρέπει να οριστεί στο **GDPR-DOC-15** για τις βασικές υπηρεσιακές διαδικασίες που προβλέπουν την προστασία των προσωπικών δεδομένων.
2.2.2.4	Θα πρέπει να εξεταστεί μια εναλλακτική δυνατότητα, ανάλογα με την οργάνωση και την αποδεκτή διακοπή του συστήματος πληροφορικής.
	Related to ISO 27001:2013 - A. 17 Information security aspects of business continuity management

3.3 Ανθρώπινοι πόροι

3.3.1 Εμπιστευτικότητα του προσωπικού

Προκειμένου να διασφαλιστεί η εμπιστευτικότητα των προσωπικών δεδομένων σύμφωνα με το άρθ. 32, ο **Δήμος Κιλκίς** θα πρέπει να διασφαλίσει ότι οι υπάλληλοί του παρέχουν επίσης επαρκείς εγγυήσεις εμπιστευτικότητας, τόσο όσον αφορά την τεχνική εμπειρογνωμοσύνη όσο και την προσωπική ακεραιότητα. Επιπλέον, σύμφωνα με το άρθρο 32.4. «Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους ».

2.3.1.1	Η **PROSET** προτείνει στο έγγραφο ***GDPR-DOC-32 Σύνοψη Πολιτικής Αποδεκτής Χρήσης*** την πολιτική δέσμευσης του προσωπικού για την διασφάλιση της εμπιστευτικότητας και ακεραιότητας των προσωπικών δεδομένων και γενικότερα των πληροφοριών. Η πολιτική αυτή πρέπει να εγκριθεί από την Διοίκηση

2.3.1.2	Ο **Δήμος Κιλκίς** πρέπει να διασφαλίζει ότι όλοι οι εργαζόμενοι κατανοούν τις ευθύνες και τις υποχρεώσεις τους σχετικά με την επεξεργασία των προσωπικών δεδομένων. Οι ρόλοι και οι ευθύνες πρέπει να κοινοποιούνται με σαφήνεια κατά τη διάρκεια της διαδικασίας πρόσληψης και / ή απασχόλησης.
2.3.1.3	Πριν από την ανάληψη των καθηκόντων τους, οι εργαζόμενοι πρέπει να κληθούν να επανεξετάσουν και να συμφωνήσουν στην πολιτική ασφάλειας του οργανισμού και να υπογράψουν αντίστοιχες συμφωνίες εμπιστευτικότητας και μη αποκάλυψης.
2.3.1.4	Οι εργαζόμενοι που εμπλέκονται σε επεξεργασία δεδομένων προσωπικού χαρακτήρα με υψηλό κίνδυνο πρέπει να δεσμεύονται από ειδικές ρήτρες εμπιστευτικότητας (βάσει της σύμβασης εργασίας ή άλλης νομικής πράξης).
	Related to ISO 27001:2013 - A.7 Human resource security

3.3.2 Εκπαίδευση

Βασική εκπαίδευση

Η εκπαίδευση του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων και συμμόρφωσης στο GDPR, καθώς και σε ειδικά θέματα σχετικά με την ασφάλεια του πληροφοριακού συστήματος (πχ. χρήση μη προβλέψιμων κωδικών πρόσβασης και συνθηματικών, τρόπο εντοπισμού και αναφοράς των περιστατικών παραβίασης της ασφαλείας, σωστή χρήση των e-mail και των αποσπωμένων μέσων αποθήκευσης, εκτίμηση του αντικτύπου) είναι ιδιαιτέρως σημαντική για την ορθή εφαρμογή των οργανωτικών και τεχνικών μέτρων ασφαλείας. Οι πληροφορίες σχετικά με τις συγκεκριμένες νομικές υποχρεώσεις όσον αφορά την προστασία δεδομένων είναι επίσης κεντρικές, ιδίως για το βασικό προσωπικό που εμπλέκεται σε επεξεργασία δεδομένων προσωπικού χαρακτήρα υψηλού κινδύνου

Η εκπαίδευση κατά την πρόσληψη πρέπει να περιλαμβάνει κατ' ελάχιστο την κοινοποίηση στους εργαζόμενους της πολιτικής ασφαλείας, για την οποία πρέπει κατά το δυνατόν να διαπιστωθεί ότι είναι πλήρως κατανοητή από όλους, καθώς επίσης και των διαδικασιών διαχείρισης περιστατικών παραβίασης δεδομένων και ανάκαμψης από καταστροφές, εφόσον άπτονται των αρμοδιοτήτων τους.

Η εκπαίδευση και ευαισθητοποίηση των χρηστών σε θέματα προστασίας προσωπικών δεδομένων θα πρέπει να περιλαμβάνει:

- Θεμελιώδης Δομές του Γενικού Κανονισμού και Ορολογία
- Δικαιώματα και Ελευθερίες των Υποκειμένων
- Διαχείριση των αιτήσεων πρόσβασης των υποκειμένων
- Συμμόρφωση με τον Νέο Κανονισμό
- Επιπτώσεις στην προστασία των προσωπικών δεδομένων
- Αναφορά περιστατικών ασφαλείας
- Διαδικασίες και πολιτικές προστασίας προσωπικών δεδομένων
- Μεταφορές προσωπικών δεδομένων εντός και εκτός της ΕΕ

Σκόπιμο θα ήταν να υπάρχει υπηρεσιακός δικτυακός τόπος (webportal) στον οποίον θα είναι αναρτημένη η περιγραφή των βασικών διαδικασιών ασφαλείας που πρέπει να γνωρίζουν τα μέλη του προσωπικού.

Θα πρέπει επίσης η εκπαίδευση να συνεχίζεται και μετά την πρόσληψη, είτε σε σημαντικές αλλαγές των διαδικασιών ασφαλείας είτε κατά την εμφάνιση σημαντικών θεμάτων ασφαλείας. Επίσης, ως προς το σκοπό της εκπαίδευσης κρίνεται σκόπιμη η κατάρτιση ειδικότερων ενημερωτικών εντύπων.

.**Εξειδικευμένη εκπαίδευση**

Πρέπει να παρέχεται στο προσωπικό που έχει αναλάβει τη διαχείριση της ασφάλειας διαρκής εξειδικευμένη εκπαίδευση σχετικά με τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών.

2.3.2.1	Η **PROSET** προτείνει το περιεχόμενο της εκπαίδευσης που βρίσκεται στα έγγραφα: • ***GDPR-DOC-02 Παρουσίαση ενημέρωσης GDPR*** • ***GDPR-DOC-12 Εκπαίδευση Ευαισθητοποίησης για την Ασφάλεια Πληροφοριών***
2.3.2.2	Ο **Δήμος Κιλκίς** πρέπει να διασφαλίσει ότι όλοι οι εργαζόμενοι ενημερώνονται επαρκώς σχετικά με τους ελέγχους ασφαλείας του συστήματος ΤΠ που σχετίζονται με την καθημερινή τους εργασία. Οι εργαζόμενοι που συμμετέχουν στην επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει επίσης να ενημερώνονται δεόντως σχετικά με τις σχετικές απαιτήσεις προστασίας δεδομένων και τις νομικές υποχρεώσεις μέσω τακτικών εκστρατειών ευαισθητοποίησης.
2.3.2.3	Ο **Δήμος Κιλκίς** θα πρέπει να διαθέτει δομημένα και τακτικά προγράμματα κατάρτισης για το προσωπικό, συμπεριλαμβανομένων ειδικών προγραμματιστών για την εισαγωγή (σε θέματα προστασίας δεδομένων) των νεοεισερχομένων.
2.3.2.4	Ένα σχέδιο κατάρτισης με καθορισμένους σκοπούς και στόχους πρέπει να προετοιμάζεται και να εκτελείται σε ετήσια βάση.
	Related to ISO 27001:2013 - A.7.2.2 Information security awareness, education and training

4 Τεχνολογικά μέτρα ασφάλειας

4.1 Έλεγχος πρόσβασης και ταυτότητας

Ο έλεγχος πρόσβασης και ο έλεγχος ταυτότητας αποτελούν βασικά μέτρα ασφαλείας για την προστασία από μη εξουσιοδοτημένη πρόσβαση στο σύστημα πληροφορικής που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων..

3.1.1	Η **PROSET** προτείνει την πολιτική ελέγχου πρόσβασης του οργανισμού ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων*** (βλ.Επίσης***2.1.3 του παρόντος εγγράφου)*** που πρέπει να ισχύει για εξοπλισμό και λογισμικό. Η πολιτική αυτή πρέπει να εγκριθεί από την Διοίκηση και να ισχύει για όλους τους χρήστες
3.1.2	Πρέπει να αποφεύγεται η χρήση κοινών λογαριασμών χρηστών. Σε περιπτώσεις όπου αυτό είναι απαραίτητο, θα πρέπει να διασφαλιστεί ότι όλοι οι χρήστες του κοινού λογαριασμού έχουν τους ίδιους ρόλους και ευθύνες
3.1.3	Οι κωδικοί πρόσβασης των χρηστών πρέπει να αποθηκεύονται σε μια φόρμα τύπου "hash".
3.1.4	Ο έλεγχος ταυτότητας συσκευής πρέπει να χρησιμοποιείται για να διασφαλίζεται ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται μόνο μέσω συγκεκριμένων πόρων του δικτύου.
	Related to ISO 27001:2013 - A.9 Access control

4.2 Καταγραφή και παρακολούθηση (Logfiles)

Η χρήση των αρχείων καταγραφής καθώς και η καταγραφή σε πίνακες βάσης δεδομένων είναι ένα βασικό μέτρο ασφάλειας που επιτρέπει τον εντοπισμό και την παρακολούθηση των ενεργειών των χρηστών (όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα), υποστηρίζοντας έτσι την λογοδοσία σε περίπτωση μη εξουσιοδοτημένης αποκάλυψης, τροποποίησης ή καταστροφής προσωπικών δεδομένων. Η παρακολούθηση των αρχείων ή και των πινάκων βάσεων δεδομένων καταγραφής είναι σημαντική για τον εντοπισμό πιθανών εσωτερικών ή εξωτερικών προσπαθειών για παραβίαση συστήματος.

3.2.1	Τα αρχεία ή και οι πίνακες καταγραφής θα πρέπει να ενεργοποιούνται για κάθε σύστημα / εφαρμογή που χρησιμοποιείται για την επεξεργασία των προσωπικών δεδομένων. Πρέπει να περιλαμβάνουν όλους τους τύπους πρόσβασης στα δεδομένα (προβολή, τροποποίηση, διαγραφή) και να εφαρμόζεται η πολιτική για τα *Αρχεία και πληροφορίες καταγραφής* που περιγράφεται στο έγγραφο ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων***.
3.2.2	Τα αρχεία ή και οι πίνακες καταγραφής πρέπει να φέρουν χρονική σήμανση και να προστατεύονται επαρκώς από τυχόν παρεμβάσεις και μη εξουσιοδοτημένη πρόσβαση. Τα ρολόγια θα πρέπει να συγχρονίζονται με μία μόνο πηγή χρόνου αναφοράς

3.2.3	Πρέπει να καταγράφονται οι ενέργειες των διαχειριστών συστημάτων και των χειριστών συστημάτων, συμπεριλαμβανομένης της προσθήκης / διαγραφής / αλλαγής δικαιωμάτων χρήστη.
3.2.4	Δεν πρέπει να υπάρχει δυνατότητα διαγραφής ή τροποποίησης του περιεχομένου των αρχείων καταγραφής. Η πρόσβαση στα αρχεία καταγραφής θα πρέπει επίσης να καταγράφεται εκτός από την παρακολούθηση για την ανίχνευση ασυνήθιστης δραστηριότητας. Πρόσβαση θα πρέπει να έχουν αποκλειστικά οι διαχειριστές των συστημάτων.
3.2.5	Ένα σύστημα παρακολούθησης πρέπει να επεξεργάζεται τα αρχεία καταγραφής και να εκπονεί αναφορές σχετικά με την κατάσταση του συστήματος και να ειδοποιεί για πιθανούς συναγερμούς.
	Related to ISO 27001:2013 - A.12.4 Logging and monitoring

4.3 Ασφάλεια των δεδομένων κατά την αποθήκευση

Τα δεδομένα σε κατάσταση ηρεμίας είναι δεδομένα που δεν μετακινούνται ενεργά από συσκευή σε συσκευή ή δίκτυο σε δίκτυο, όπως τα αποθηκευμένα δεδομένα σε σκληρό δίσκο, φορητό υπολογιστή, μονάδα flash ή αρχειοθετημένα / αποθηκευμένα με κάποιο άλλο τρόπο. Ως εκ τούτου, αυτή η κατηγορία μέτρων σχετίζεται κυρίως με την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε βάσεις δεδομένων ή άλλα συναφή συστήματα (συμπεριλαμβανομένης της αποθήκευσης σε νέφος). Αφορά επίσης την επεξεργασία προσωπικών δεδομένων από τους εργαζομένους με τη χρήση συγκεκριμένων σταθμών εργασίας ή άλλων συσκευών. Το GDPR αναγνωρίζει την ικανότητα της ψευδωνυμοποίησης για να βοηθήσει στην προστασία των δικαιωμάτων των ατόμων, ενώ παράλληλα επιτρέπει την χρησιμότητα των δεδομένων. Σύμφωνα με το άρθρο 32, ένα από τα μέτρα που αναφέρονται είναι η "ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα". Το προτεινόμενο μέτρο είναι η κρυπτογράφηση αρχείων και δεδομένων προσωπικού χαρακτήρα η οποία θα πρέπει θα πρέπει να εφαρμόζεται και να ακολουθεί την πολιτική ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων***

4.4 Ασφάλεια Διακομιστή (server)/Βάσης Δεδομένων

Οι διακομιστές και οι βάσεις δεδομένων αποτελούν τη ραχοκοκαλιά του συστήματος επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Πρέπει να είναι ασφαλείς για να εξασφαλίσουν ένα ασφαλές περιβάλλον λειτουργίας. Θα πρέπει να ακολουθείται η πολιτική ελέγχου πρόσβασης διακομιστή και εφαρμογών που περιγράφεται στο έγγραφο οργανισμού ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων***

3.4.1	Οι servers βάσεων δεδομένων και εφαρμογών θα πρέπει να ρυθμιστούν ώστε να εκτελούνται χρησιμοποιώντας διακριτούς λογαριασμούς χρηστών με τα ελάχιστα δικαιώματα που απαιτούνται στο λειτουργικό σύστημα (αρχή των ελαχίστων δικαιωμάτων).
3.4.2	Οι διακομιστές βάσεων δεδομένων και εφαρμογών θα πρέπει να επεξεργάζονται μόνο τα προσωπικά δεδομένα που πραγματικά χρειάζονται για επεξεργασία, προκειμένου να επιτύχουν τους σκοπούς επεξεργασίας τους.
3.4.3	Οι λύσεις κρυπτογράφησης πρέπει να εξετάζονται σε συγκεκριμένα αρχεία ή φακέλους που περιέχουν προσωπικά δεδομένα χρησιμοποιώντας κατάλληλα προγράμματα (πχ. Λογισμικά VeraCrypt ή Zed! ή χρησιμοποιώντας το EFS των windows)
3.4.4	Πρέπει να λαμβάνεται υπόψη η κρυπτογράφηση των μονάδων αποθήκευσης
3.4.5	Οι τεχνικές ψευδωνυμοποίησης στην βάση δεδομένων , αν επιλεγούν, θα πρέπει να εφαρμόζονται μέσω του διαχωρισμού των δεδομένων από τα άμεσα αναγνωριστικά στοιχεία ώστε να αποφεύγεται η σύνδεση με το υποκείμενο των δεδομένων χωρίς πρόσθετες πληροφορίες. Περισσότερες πληροφορίες για τις τεχνικές μπορούν να βρεθούν από την ομάδα W29: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_el.pdf
3.4.6	Θα πρέπει να λαμβάνονται υπόψη τεχνικές που υποστηρίζουν την προστασία της ιδιωτικότητας σε επίπεδο βάσης δεδομένων, όπως εξουσιοδοτημένα ερωτήματα με βάση τη διαβάθμιση των χρηστών, ερωτήματα για τη διατήρηση της ιδιωτικότητας των βάσεων δεδομένων (πχ. έλεγχος δικαιωμάτων κατά την εξαγωγή δεδομένων μέσω εκτυπώσεων (αποστολή σε pdf κλπ.) και διαβάθμιση των δεδομένων (data classification)) καθώς και κρυπτογράφηση των δεδομένων με δυνατότητα αναζήτησης.
3.4.7	Θα πρέπει να υπάρχει ένας backup server με εγκατεστημένες τις κρίσιμες υπηρεσιακές εφαρμογές τελευταίας έκδοσης. Ο backup server παραμένει κλειστός, λειτουργεί περιοδικά για να είναι πάντα αναβαθμισμένες στην τελευταία έκδοση οι εφαρμογές. Σε περίπτωση μη διαθεσιμότητας του κυρίως server (καταστροφή του εξοπλισμού, επίθεση ransomware κρυπτογράφησης) να χρησιμοποιηθεί αφού ανακληθούν τα δεδομένα των εφαρμογών από το τελευταίο ασφαλές backup
	Related to ISO 27001:2013 - A. 12 Operations security

4.5 Ασφάλεια του σταθμού εργασίας

Αυτό το μέτρο σχετίζεται κυρίως με τη διαμόρφωση ασφαλείας των σταθμών εργασίας των χρηστών ή άλλων συσκευών. είναι σημαντικό να επιβάλλονται συγκεκριμένες πολιτικές ασφαλείας και να περιορίζονται οι χρήστες από την εκτέλεση ορισμένων ενεργειών που θα μπορούσαν να θέσουν σε κίνδυνο την

ασφάλεια του συστήματος πληροφορικής (πχ. απενεργοποίηση προγραμμάτων προστασίας από ιούς ή εγκατάσταση μη εξουσιοδοτημένου λογισμικού).Θα πρέπει να ακολουθείται η γενική πολιτική πρόσβασης στα πληροφορικά συστήματα που περιγράφεται στο έγγραφο οργανισμού ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων.***

3.5.1	Οι χρήστες δεν θα πρέπει να μπορούν να απενεργοποιούν ή να παρακάμπτουν τις ρυθμίσεις ασφαλείας.
3.5.2	Οι εφαρμογές προστασίας από ιούς και οι υπογραφές ανίχνευσης πρέπει να διαμορφώνονται σε εβδομαδιαία βάση.
3.5.3	Οι χρήστες δεν θα πρέπει να έχουν δικαιώματα για να εγκαταστήσουν ή να απενεργοποιήσουν μη εξουσιοδοτημένες εφαρμογές λογισμικού.
3.5.4	Το σύστημα θα πρέπει να έχει χρονικά διαστήματα σύνδεσης, όταν ο χρήστης δεν είναι ενεργός για μια συγκεκριμένη χρονική περίοδο.
3.5.5	Οι κρίσιμες ενημερώσεις ασφαλείας που κυκλοφορούν από τον κατασκευαστή του λειτουργικού συστήματος θα πρέπει να εγκαθίστανται τακτικά.
3.5.6	Οι εφαρμογές κατά των ιών και οι υπογραφές ανίχνευσης πρέπει να ρυθμίζονται καθημερινά.
3.5.7	Δεν πρέπει να επιτρέπεται η μεταφορά προσωπικών δεδομένων από σταθμούς εργασίας σε εξωτερικές συσκευές αποθήκευσης (πχ. USB, DVD, εξωτερικοί σκληροί δίσκοι).
3.5.8	Οι σταθμοί εργασίας που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων δεν πρέπει κατά προτίμηση να συνδέονται με το Διαδίκτυο, εκτός εάν υπάρχουν μέτρα ασφαλείας για την αποτροπή της μη εξουσιοδοτημένης επεξεργασίας, αντιγραφής και μεταφοράς δεδομένων προσωπικού χαρακτήρα στον χώρο.
3.5.9	Πρέπει να ενεργοποιηθεί η κρυπτογράφηση λογισμικού πλήρους δίσκου στις μονάδες λειτουργικού συστήματος του σταθμού εργασίας
3.5.10	Όλοι οι χρήστες πρέπει να λειτουργούν με λογαριασμούς απλού χρήστη και όχι διαχειριστή. Ακόμα και οι διαχειριστές των συστημάτων προτείνεται να μην χρησιμοποιούν τους λογαριασμούς διαχειριστή, παρά μόνο όταν είναι απολύτως απαραίτητο.
	Related to ISO 27001:2013 - A. 14.1 Security requirements of information systems

4.6 Ασφάλεια Δικτύου/Επικοινωνίας

Η ασφάλεια του δικτύου είναι σημαντική για την προστασία των προσωπικών δεδομένων, τόσο όσον αφορά τις εξωτερικές συνδέσεις (πχ. στο Διαδίκτυο), όσο και τη διασύνδεση με άλλα συστήματα (εξωτερικά ή εσωτερικά) του Δήμου Κιλκίς.

3.6.1	Κάθε φορά που γίνεται πρόσβαση μέσω του Διαδικτύου, η επικοινωνία πρέπει να κρυπτογραφείται μέσω κρυπτογραφικών πρωτοκόλλων (TLS / SSL).
3.6.2	Η ασύρματη πρόσβαση στο σύστημα πληροφορικής θα πρέπει να επιτρέπεται μόνο για συγκεκριμένους χρήστες και διαδικασίες. Πρέπει να προστατεύεται με μηχανισμούς κρυπτογράφησης.
3.6.3	Η απομακρυσμένη πρόσβαση στο σύστημα πληροφορικής θα πρέπει γενικά να αποφεύγεται. Σε περιπτώσεις όπου αυτό είναι απολύτως απαραίτητο, θα πρέπει να εκτελείται μόνο υπό τον έλεγχο και την παρακολούθηση συγκεκριμένου ατόμου από τον οργανισμό (πχ. διαχειριστής IT / υπεύθυνος ασφαλείας) μέσω προκαθορισμένων συσκευών.
3.6.4	Η κυκλοφορία προς και από το σύστημα πληροφορικής θα πρέπει να παρακολουθείται και να ελέγχεται μέσω των Συστημάτων Firewalls ή και των Συστημάτων Ανίχνευσης Εισβολών. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny)
3.6.5	Το δίκτυο του συστήματος πληροφοριών πρέπει να διαχωρίζεται από τα άλλα δίκτυα του υπεύθυνου επεξεργασίας δεδομένων.
3.6.6	Η πρόσβαση στο σύστημα πληροφορικής θα πρέπει να πραγματοποιείται μόνο από προεγκεκριμένες συσκευές και τερματικό χρησιμοποιώντας τεχνικές όπως το φιλτράρισμα MAC ή το Network Access Control (NAC)
3.6.7	Η απομακρυσμένη πρόσβαση των εξωτερικών τεχνικών υποστήριξης του λογισμικού και των μηχανημάτων θα πρέπει να ακολουθεί την πολιτική απομακρυσμένης σύνδεσης που περιγράφεται στο ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων***
	Related to ISO 27001:2013 - A.13 Communications Security

4.7 Αντίγραφα ασφαλείας (Backups)

Ένα σύστημα δημιουργίας αντιγράφων ασφαλείας αποτελεί ουσιαστικό μέσο για την ανάκτηση από την απώλεια ή την καταστροφή δεδομένων. Ενώ πρέπει να υπάρχει κάποιο σύστημα, η συχνότητα και η φύση της δημιουργίας αντιγράφων ασφαλείας θα εξαρτηθεί, μεταξύ άλλων, από τον τύπο της οργάνωσης και τη φύση των δεδομένων που υποβάλλονται σε επεξεργασία. Σύμφωνα με το άρθρο

32 του GDPR, η πτυχή της «ικανότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε προσωπικά δεδομένα» σε μέρος των υποχρεώσεων ασφάλειας δεδομένων για τον υπεύθυνο επεξεργασίας δεδομένων ή τον επεξεργαστή δεδομένων.

3.7.1	Οι διαδικασίες δημιουργίας αντιγράφων ασφαλείας και αποκατάστασης στοιχείων θα πρέπει να καθορίζονται, να τεκμηριώνονται και να συνδέονται σαφώς με τους ρόλους και τις ευθύνες.
3.7.2	Για τα αντίγραφα ασφαλείας θα πρέπει να παρέχεται το κατάλληλο επίπεδο φυσικής και περιβαλλοντικής προστασίας σύμφωνα με τα πρότυπα που εφαρμόζονται στα αρχικά δεδομένα.
3.7.3	Η εκτέλεση των αντιγράφων ασφαλείας θα πρέπει να παρακολουθείται για να εξασφαλιστεί η πληρότητα.
3.7.4	Τα αντίγραφα ασφαλείας θα πρέπει να δημιουργούνται σύμφωνα με την πολιτική Δημιουργίας αντιγράφων ασφαλείας που περιγράφεται στο ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων***.
3.7.5	Τα εφεδρικά μέσα θα πρέπει να ελέγχονται τακτικά ώστε να διασφαλίζεται ότι μπορούν να χρησιμοποιηθούν σε περίπτωση ανάγκης ανάκτησης δεδομένων.
3.7.6	Αντίγραφα του αντιγράφου ασφαλείας θα πρέπει να αποθηκεύονται με ασφάλεια σε διαφορετικές φυσικές τοποθεσίες.
3.7.7	Σε περίπτωση που χρησιμοποιείται υπηρεσία τρίτου μέρους για αποθήκευση αντιγράφων ασφαλείας, το αντίγραφο πρέπει να κρυπτογραφηθεί πριν μεταδοθεί/μεταφερθεί από τον υπεύθυνο επεξεργασίας δεδομένων.
3.7.8	Προτείνεται η προετοιμασία ενός ολοκληρωμένου Σχεδίου Ανάκτησης από Καταστροφή
	Related to ISO 27001:2013 - A.12.3 Back-Up

4.8 Εξοπλισμός κινητής τηλεφωνίας/φορητά

Οι φορητές / φορητές συσκευές μπορούν να επεκτείνουν το επίπεδο των υπηρεσιών που προσφέρει ο υπεύθυνος επεξεργασίας δεδομένων, αλλά να αυξήσουν την έκθεση σε κλοπή και τυχαία απώλεια. Στην περίπτωση κινητών συσκευών, όπως smartphones ή tablet, οι χρήστες μπορούν επίσης να τις εφαρμόσουν για προσωπική χρήση και πρέπει να δοθεί ιδιαίτερη προσοχή ώστε να μην παραβιάζονται τα υπηρεσιακά δεδομένα.

3.8.1	Οι διαδικασίες διαχείρισης κινητών και φορητών συσκευών θα πρέπει να καθοριστούν και να τεκμηριωθούν, προβλέποντας σαφείς κανόνες για τη σωστή χρήση τους.
3.8.2	Οι κινητές συσκευές που επιτρέπεται να έχουν πρόσβαση στο σύστημα πληροφοριών πρέπει να είναι προκαταχωρισμένες και προεγκεκριμένες.
3.8.3	Οι κινητές συσκευές πρέπει να υπόκεινται στα ίδια επίπεδα διαδικασιών ελέγχου πρόσβασης (στο σύστημα επεξεργασίας δεδομένων) ως άλλος τερματικός εξοπλισμός.
3.8.4	Οι συγκεκριμένοι ρόλοι και ευθύνες όσον αφορά τη διαχείριση κινητών και φορητών συσκευών θα πρέπει να καθοριστούν σαφώς.
3.8.5	Ο οργανισμός θα πρέπει να είναι σε θέση να διαγράφει εξ αποστάσεως προσωπικά δεδομένα (που σχετίζονται με τη λειτουργία επεξεργασίας) σε κινητή συσκευή που έχει παραβιαστεί.
3.8.6	Οι κινητές συσκευές πρέπει να υποστηρίζουν τον διαχωρισμό της ιδιωτικής και επαγγελματικής χρήσης της συσκευής μέσω ασφαλών εφαρμογών λογισμικού.
3.8.7	Οι κινητές συσκευές πρέπει να προστατεύονται φυσικά από κλοπή όταν δεν χρησιμοποιούνται.
3.8.8	Θα πρέπει να λαμβάνεται υπόψη ο έλεγχος ταυτότητας δύο παραγόντων για την πρόσβαση σε κινητές συσκευές καθώς και να εξεταστεί το ενδεχόμενο κρυπτογράφησης τους
3.8.9	Τα προσωπικά δεδομένα που είναι αποθηκευμένα στην κινητή συσκευή (ως μέρος της λειτουργίας επεξεργασίας δεδομένων του οργανισμού) θα πρέπει να κρυπτογραφούνται.
	Related to ISO 27001:2013 - A. 6.2 Mobile devices and teleworking

4.9 Διαγραφή δεδομένων

Ο σκοπός της διαγραφής είναι η μη αναστρέψιμη κατάσταση ή καταστροφή των προσωπικών δεδομένων ώστε να μην είναι δυνατή η ανάκτηση. Κατά συνέπεια, η χρησιμοποιούμενη μέθοδος πρέπει να ταιριάζει με τον τύπο της τεχνολογίας αποθήκευσης, συμπεριλαμβανομένων των αντιγράφων που βασίζονται σε χαρτί. Κατά τη παραχώρηση του παρωχημένου ή περιττού εξοπλισμού, ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίσει ότι όλα τα δεδομένα που είχαν προηγουμένως αποθηκευτεί στις συσκευές έχουν αφαιρεθεί πριν από τη διάθεσή τους. Σύμφωνα με το άρθρο 6, τα προσωπικά δεδομένα GDPR δεν πρέπει να διατηρούνται για περισσότερο από ό,τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή για τους οποίους υποβάλλονται σε περαιτέρω επεξεργασία. Σε ορισμένες περιπτώσεις, τα υποκείμενα δεδομένων

έχουν επίσης το δικαίωμα να ζητήσουν διαγραφή πριν από τη λήξη της μέγιστης περιόδου διατήρησης και στα οποία θα πρέπει να δοθεί η κατάλληλη απάντηση.

3.9.1	Η διαγραφή/αντικατάσταση των δεδομένων βασισμένη στο λογισμικό πρέπει να εκτελείται σε όλα τα μέσα πριν από τη διάθεσή τους. Σε περιπτώσεις όπου αυτό δεν είναι εφικτό (CD, DVD, κλπ.) πρέπει να πραγματοποιηθεί φυσική καταστροφή.
3.9.2	Πραγματοποιείται τεμαχισμός χαρτιού με καταστροφέα εγγράφων τύπου κοπής κομφετί και φορητών μέσων που χρησιμοποιούνται για την αποθήκευση δεδομένων προσωπικού χαρακτήρα.
3.9.3	Πολλά περάσματα τυχαίων δεδομένων στα Sectors του δίσκου, με εξειδικευμένη τεχνική βασισμένη στο λογισμικό που αποτρέπει ακόμα και ανεύρεση δεδομένων από εταιρίες ανάκτησης δεδομένων, πρέπει να εκτελούνται σε όλα τα μέσα αποθήκευσης πριν από τη διάθεσή τους.
3.9.4	Εάν οι υπηρεσίες τρίτου μέρους χρησιμοποιούνται για ασφαλή διαγραφή μέσων ή εγγράφων που βασίζονται σε χαρτί, θα πρέπει να υπάρχει μια συμφωνία παροχής υπηρεσιών και να καταρτίζεται καταγραφή καταστροφής των αρχείων ανάλογα με την περίπτωση.
3.9.5	Μετά τη διαγραφή από το λογισμικό, θα πρέπει να εκτελεστούν πρόσθετα μέτρα που βασίζονται στο υλικό, όπως η απομαγνήτηση του μέσου. Ανάλογα με την περίπτωση, θα πρέπει επίσης να εξεταστεί η φυσική καταστροφή.
3.9.6	Εάν ένα τρίτο μέρος, ως εκ τούτου εκτελών την επεξεργασία, χρησιμοποιείται για την καταστροφή μέσων ή έντυπων αρχείων, θα πρέπει να θεωρείται ότι η διαδικασία πραγματοποιείται στις εγκαταστάσεις του υπεύθυνου επεξεργασίας δεδομένων (και αποφεύγεται η μεταφορά προσωπικών δεδομένων εκτός τόπου.
	Related to ISO 27001:2013 - A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re- use of equipment

4.10 Φυσική Ασφάλεια

Η φυσική ασφάλεια είναι εξίσου σημαντική για τα μέτρα ασφάλειας που προσανατολίζονται στην τεχνολογία, καθώς η φυσική πρόσβαση στο σύστημα πληροφοριών μπορεί να αποτελέσει τη βάση για τη συνολική στρατηγική ασφάλειας

3.10.1	Ο **Δήμος Κιλκίς** θα πρέπει να ακολουθεί την πολιτική για τις υποδομές φύλαξης προσωπικών δεδομένων που περιγράφεται στο ***GDPR-DOC-16 Πολιτική Διατήρησης και Προστασίας Δεδομένων***

3.10.2	Ο φυσικός χώρος που φιλοξενεί τους διακομιστές (servers), τον τηλεπικοινωνιακό και δικτυακό εξοπλισμό δεν πρέπει να είναι προσβάσιμος από μη εξουσιοδοτημένο προσωπικό.
3.10.3	Οι ασφαλείς ζώνες θα πρέπει να ορίζονται και να προστατεύονται από τα κατάλληλα χειριστήρια εισόδου. Ένα φυσικό ημερολόγιο ή ένα ηλεκτρονικό ίχνος ελέγχου όλων των προσβάσεων θα πρέπει να διατηρείται και να παρακολουθείται με ασφάλεια
3.10.4	Τα συστήματα ανίχνευσης εισβολέων πρέπει να εγκαθίστανται σε όλες τις ζώνες ασφαλείας.
3.10.5	Οι κενές ασφαλείς περιοχές θα πρέπει να κλειδώνονται φυσικά και να επανεξετάζονται περιοδικά
3.10.6	Ένα αυτόματο σύστημα καταστολής πυρκαγιάς, το κλειστό σύστημα ελέγχου κλιματισμού και η αδιάλειπτη παροχή ρεύματος (UPS) θα πρέπει να εφαρμοστούν στην αίθουσα εξυπηρετητών (servers)
3.10.7	Το προσωπικό υποστήριξης των εξωτερικών συνεργατών πρέπει να διαθέτει περιορισμένη πρόσβαση σε ασφαλείς περιοχές.
	Related to ISO 27001:2013 - A.11 – Physical and environmental security

4.11 Ασφάλεια του φυσικού αρχείου

Για τους χώρους όπου υπάρχει Φυσικό Αρχείο θα πρέπει τουλάχιστον να ληφθούν τα εξής μέτρα:

3.11.1	Κάθε χώρος θα πρέπει να παραμένει κλειδωμένος όσο δεν υπάρχει υπεύθυνος ή εργαζόμενος που να ελέγχει τον χώρο.
3.11.2	Θετικό είναι να υπάρχει σύστημα ελέγχου πρόσβασης, όπως ειδικές μαγνητικές κλειδαριές και αναγνώστες καρτών ασφαλείας για την είσοδο στον χώρο. Η πρόσβαση στον χώρο θα πρέπει να καταγράφεται
3.11.3	Θα πρέπει να υπάρχει σύστημα πυρανίχνευσης
3.11.4	Τα βιβλία, τα τετράδια και οι σκληροί δίσκοι θα πρέπει να είναι σε συρτάρια ή ντουλάπες κλειδωμένα όσο χρόνο δεν χρησιμοποιούνται

4.12 Χρήση ηλεκτρονικού ταχυδρομείου για αποστολή προσωπικών δεδομένων

Η χρήση του ηλεκτρονικού ταχυδρομείου για την αποστολή προσωπικών δεδομένων στα υποκείμενα των δεδομένων και σε τρίτους θα πρέπει να είναι ασφαλής.

3.12.1	Θα πρέπει να γίνεται πάντα επαλήθευση του παραλήπτη. Προσέχετε τη δυνατότητα αυτόματης συμπλήρωσης ορισμένων πελατών ηλεκτρονικού ταχυδρομείου, όπου το σύστημα προτείνει παραλήπτες με βάση τους χαρακτήρες που έχουν πληκτρολογηθεί μέχρι στιγμής.
3.12.2	Να μη διακινούνται προσωπικά δεδομένα μέσω ηλεκτρονικού ταχυδρομείου, δίχως να γίνεται χρήση κρυπτογραφικών μεθόδων. Τα κλειδιά ή οι κωδικοί πρέπει να αποστέλλονται από άλλο κανάλι όπως με sms. Μπορεί επίσης να επιλεγεί η χρήση ψηφιακών πιστοποιητικών για την ασύμμετρη κρυπτογράφηση όταν είναι εφικτό
3.12.3	Θα μπορεί κάθε χρήστης που στέλνει ή παραλαμβάνει email με προσωπικά δεδομένα να έχει εγκατεστημένο στον προσωπικό του υπολογιστή μια client-email εφαρμογή (πχ outlook, Thunderbird) με δυνατότητες κρυπτογράφησης ή εφαρμογή κρυπτογράφησης (πχ Gpg4Win). Εναλλακτικά το περιεχόμενο του email μπορεί να συμπιέζεται και να κρυπτογραφείται με κάποιο κωδικό και στην συνέχεια να αποστέλλεται (3.12.2)
3.12.4	Δεν πρέπει να επιτρέπεται η χρήση ηλεκτρονικών μηνυμάτων που περιέχουν προσωπικά δεδομένα σε προσωπικές ηλεκτρονικές θυρίδες
3.12.5	Απαγορεύεται η αποστολή λογαριασμού και συνθηματικού
3.12.6	Σε περίπτωση αποστολής ηλεκτρονικής αλληλογραφίας σε παραπάνω από έναν αποδέκτες (και εφόσον δεν είναι απαραίτητη η μεταξύ τους επικοινωνία) προτείνεται η χρήση του πεδίου της κρυφής κοινοποίησης για την εισαγωγή των παραληπτών.

4.13 Ελαχιστοποίηση δεδομένων

Ο GDPR εισάγει την έννοια της ελαχιστοποίησης των προσωπικών δεδομένων για τις διάφορες επεξεργασίες τους.

Μέτρα που μπορούν να ληφθούν προς την κατεύθυνση αυτή είναι:

1. Καταχωρούμε και αποθηκεύουμε μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για κάθε επεξεργασία. (όχι πλεονάζοντα)

2. Ρυθμίζουμε τα δικαιώματα χρηστών σε Files, Erp, Crm ώστε να έχουν πρόσβαση μόνο όσοι απαιτούνται από την επεξεργασία.
3. Πρέπει να γίνει ελαχιστοποίηση και διαχείριση των reports (xls)(ειδικά αυτών με προσωπικά δεδομένα) που διακινούνται στην υπηρεσία. Θα πρέπει να είναι συγκεκριμένα και εγκεκριμένα από DPO, Υπεύθυνος Τμήματος και Διοίκηση.
4. Ανά τμήμα να ζητηθεί ποια είναι τα απαραίτητα reports για την κάθε εργασία-διαδικασία και να μην δίνεται δυνατότητα παραγωγής νέου report χωρίς τον έλεγχο και έγκριση DPO,Υπεύθυνου Τμήματος και Διοίκησης.
5. Να διερευνηθεί η δυνατότητα (στο ERP, CRM) να μην υπάρχει η δυνατότητα για copy ή export της λίστας (xls) που περιέχει προσωπικά δεδομένα.
6. Για να μην αναπαράγονται xls με προσωπικά δεδομένα από τα συστήματα χωρίς έλεγχο, πρέπει να ορισθούν τα κατάλληλα δικαιώματα.
7. Όπου υπάρχει η δυνατότητα μεταφέρουμε ένα κωδικό και όχι όλη την Πληροφορία που περιέχει προσωπικά δεδομένα (συστήματα ERP,CRM, HRMS, Μισθοδοσία, κλπ)
8. Για τα δεδομένα που υπάρχουν σε ‘ αδράνεια’ στις βάσεις δεδομένων, πρέπει να υπάρχει διαδικασία αξιολόγησης και διαγραφής ή ελαχιστοποίησης σε ορισμένα χρονικά διαστήματα.

Υποχρεωτικά Μέτρα	**Προαιρετικά Μέτρα**

Δημιουργία Domain / Active Directory	Παρακολούθηση Log Files
Password Policy	Σύστημα ανίχνευσης Εισβολής
Anti-Virus	VPN (Εξετάζουμε τους λόγους μόνο με συγκεκριμένα μέτρα ασφάλειας και περιορισμένη χρήση)
User Policy	Ψηφιακές Υπογραφές
Backup / Restore	Monitoring Software
Software Updates(OS - Antivirus)	Ασφάλεια από ειδικότερες φυσικές καταστροφές
Κρυπτογράφηση mail και Βάσεων Δεδομένων	Κάμερες/Καταγραφικό
Ασφάλεια πρόσβασης στις επιμέρους κτιριακές εγκαταστάσεις	Access Control στις εισόδους
Ασφάλεια πρόσβασης ΠΣ εξοπλισμού	Σύστημα ειδοποίησης Περιβαλλοντικών συνθηκών
Πυρασφάλεια	
Συναγερμός	
Περιορισμός & Διαχωρισμός WiFi	
Κλείδωμα θυρών USB/CD-ROM/DVD	
Ελαχιστοποίηση δεδομένων στα Πληροφοριακά Συστήματα	
Σχέδιο Ανάκτησης από Καταστροφή	