ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΥΠΗΡΕΣΙΩΝ ΕΝΑΡΜΟΝΙΣΗΣ / ΣΥΜΜΟΡΦΩΣΗΣ ΤΟΥ ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ - ΟΦΘΑΛΜΙΑΤΡΕΙΟ ΑΘΗΝΩΝ - ΠΟΛΥΚΛΙΝΙΚΗ», ΟΡΓΑΝΙΚΗ ΜΟΝΑΔΑ ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ» ΜΕ ΤΙΣ ΑΠΑΙΤΗΣΕΙΣ / ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR) 679/2016

Εισαγωγή - Αντικείμενο του έργου

Ο Κανονισμός (ΕΕ) 2016/679 «General Data Protection Regulation - GDPR», για την Προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, ετέθει σε ισχύ στις 25 Μαΐου 2016 και τέθηκε σε εφαρμογή στις 25 Μαΐου 2018.

Ο Κανονισμός έχει εφαρμογή σε όλους τους οργανισμούς (ιδιωτικούς και δημόσιους οργανισμούς/επιχειρήσεις, κρατικές αρχές, συλλόγους, κ.λπ.) που διαχειρίζονται , επεξεργάζονται, αποθηκεύουν και διακινούν δεδομένα προσωπικού χαρακτήρα, εφόσον τα δεδομένα αφορούν Ευρωπαίους πολίτες ή σχετίζονται με οποιουδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες.

Το ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ» είναι φορέας παροχής υπηρεσιών υγείας εξαιρετικά μεγάλης δυναμικότητας (περίπου 950 κλίνες), με μεγάλη προσέλευση και διακίνηση ασθενών είτε σε καθεστώς γενικής εφημερίας είτε σε επίπεδο τακτικών εξωτερικών ιατρείων, όπως προκύπτει από τις διαθέσιμες καταγραφές. Επίσης, απασχολεί μεγάλο αριθμό εργαζομένων. Ως εκ τούτου, επεξεργάζεται εξαιρετικά μεγάλο όγκο δεδομένων προσωπικού χαρακτήρα και πληροφορίες (σε ηλεκτρονικά και φυσικά αρχεία) που μπορούν να ταυτοποιήσουν φυσικά πρόσωπα όπως ασθενείς, εργαζομένους, συνεργάτες, προμηθευτές κ.ά..

Αντικείμενο του έργου είναι η εναρμόνιση του ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ» με τις απαιτήσεις Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 679/2016 (GDPR).

Σκοπός είναι η αναγνώριση των τεχνολογικών και οργανωτικών αναγκών του Νοσοκομείου και η κάλυψή τους με την υλοποίηση των αντίστοιχων μέτρων για την επίτευξη συνεχούς συμμόρφωσής του με τις απαιτήσεις του GDPR.

Το Έργο θα αφορά όλες τις Οργανικές/Λειτουργικές Μονάδες (τυπικές και άτυπες) και Παραρτήματα του Νοσοκομείου.

Το Έργο περιλαμβάνει τρεις (3) διακριτές υπηρεσίες, ήτοι:

Α) Υπηρεσίες Συμβούλου για την Εναρμόνιση/Συμμόρφωση του Νοσοκομείου με τις Απαιτήσεις/Προδιαγραφές του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) 679/2016,

Β) Υπηρεσίες Υπευθύνου Προστασίας Δεδομένων (DPO)

Γ) Υπηρεσία Διαχείρισης Απειλών 24x7x365 σε πραγματικό χρόνο από Εξειδικευμένο Επιχειρησιακό Κέντρο Ασφαλείας

Οι τεχνικές προδιαγραφές των ως άνω υπηρεσιών είναι οι ακόλουθες:

Α. ΥΠΗΡΕΣΙΕΣ ΣΥΜΒΟΥΛΟΥ ΓΙΑ ΤΗΝ ΕΝΑΡΜΟΝΙΣΗ ΤΟΥ ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ - ΟΦΘΑΛΜΙΑΤΡΕΙΟ ΑΘΗΝΩΝ - ΠΟΛΥΚΛΙΝΙΚΗ», ΟΡΓΑΝΙΚΗ ΜΟΝΑΔΑ ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ» ΜΕ ΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR) 679/2016.

Τεχνική περιγραφή

Αναλυτικά το έργο θα περιλαμβάνει:

1. Ανάλυση της υφιστάμενης κατάστασης ως προς την προστασία των προσωπικών δεδομένων, η οποία θα περιλαμβάνει την αξιολόγηση των υφιστάμενων πρακτικών, των γραπτών πολιτικών και διαδικασιών, των πληροφοριακών συστημάτων και δικτυακών υποδομών, και κάθε στοιχείου που επηρεάζει την προστασία προσωπικών δεδομένων σε όλες τις δραστηριότητες και όλα τα τμήματα, παραρτήματα και Διευθύνσεις του Νοσοκομείου.

2. Ενημέρωση και συνεργασία (με συναντήσεις/συνεντεύξεις) με αρμόδια στελέχη Τμημάτων του Οργανισμού, καλύπτοντας κάθε μείζονα δραστηριότητα, τμήμα, εξωνοσοκομειακή δομή και γραφείο.
3. Δημιουργία λεπτομερών data flow maps ανά επιχειρησιακή μονάδα, τμήμα ή ανά κατηγορία προσωπικών δεδομένων, με σκοπό την επαρκή συμβατότητα με τις απαιτήσεις του GDPR, όπου θα απεικονίζονται όλες οι πληροφορίες σχετικά με τη διαχείριση των προσωπικών δεδομένων στο νοσοκομείο. Τα data flow maps θα καλύπτουν την απαίτηση του GDPR για το αρχείο δραστηριοτήτων επεξεργασίας δεδομένων και θα περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η υφιστάμενη κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να εντοπίζονται κενά ως προς τις απαιτήσεις του θεσμικού πλαισίου.
4. Εύρεση κενών ως προς την ικανοποίηση των απαιτήσεων του κανονισμού (Gap Analysis) κατηγοριοποιημένα ανά θεματική περιοχή και κρισιμότητα.
5. Ενδελεχή αξιολόγηση και σύνταξη μελέτης εκτίμησης αντικτύπου τυχόν συμβάντων παραβίασης της ιδιωτικότητας των προσωπικών δεδομένων (Data Privacy Impact Assessment) με βάση τη μεθοδολογία του ISO29134, την οδηγία της WP29 και τις υφιστάμενες οδηγίες των Ευρωπαϊκών Αρχών Προστασίας Δεδομένων.
6. Για κάθε κενό που εντοπίζεται, καθορισμός των απαραίτητων ενεργειών πρόληψης, αντιμετώπισης και δημιουργία ενός λεπτομερούς, προτεραιοποιημένου και ολοκληρωμένου πλάνου συμμόρφωσης (compliance plan and roadmap).
7. Αξιολόγηση των τρεχουσών πρακτικών επεξεργασίας προσωπικών δεδομένων και σύνταξη των απαραίτητων Πολιτικών και Διαδικασιών Προστασίας Προσωπικών Δεδομένων με βάση τα προτεινόμενα μέτρα του πλάνου συμμόρφωσης. Η ανωτέρω αξιολόγηση θα περιλαμβάνει κατ' ελάχιστο τα εξής:
    1. Αξιολόγηση της νομικής βάσης, στην οποία στηρίζεται η συλλογή του συνόλου των συλλεγόμενων προσωπικών δεδομένων, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο, των παρεχόμενων πληροφοριών κ.λπ.
    2. Αξιολόγηση της νομιμότητας και της ασφαλούς διαβίβασης προσωπικών δεδομένων

3. Αξιολόγηση του επιπέδου ωριμότητας και ευαισθητοποίησης του Νοσοκομείου στα θέματα προστασίας προσωπικών δεδομένων
4. Αξιολόγηση της δυνατότητας ικανοποίησης των δικαιωμάτων των φυσικών προσώπων
5. Αξιολόγηση της επάρκειας της οργανωτικής δομής
6. Αξιολόγηση του επιπέδου ασφαλείας και επιχειρησιακής συνέχειας
7. Αξιολόγηση των πληροφοριακών συστημάτων
8. Αξιολόγηση των συμβάσεων με τρίτους που εκτελούν επεξεργασία προσωπικών δεδομένων του οργανισμού
9. Αξιολόγηση των μέτρων προστασίας και των μηχανισμών ελέγχου και διασφάλισης της συμμόρφωσης
10. Αξιολόγηση των σχετικών γραπτών πολιτικών και διαδικασιών.

Με σκοπό την επιτυχή υλοποίηση του έργου ο υποψήφιος Ανάδοχος είναι απαραίτητο να:

1. Συμπεριλάβει ανάλυση της υφιστάμενης κατάστασης των πληροφοριακών συστημάτων και δικτυακών υποδομών και των υφιστάμενων πολιτικών, διαδικασιών και πρακτικών, οι οποίες σχετίζονται με την ασφάλεια και την προστασία των προσωπικών δεδομένων.

2. Διεξάγει συνεντεύξεις με τα αρμόδια στελέχη του νοσοκομείου καλύπτοντας κάθε δραστηριότητα αυτού.

3. Διεξάγει λεπτομερή αξιολόγηση των επιπτώσεων στην προστασία δεδομένων, βάσει του προτύπου ISO 29134, της κατευθυντήριας οδηγίας της WP29 και άλλων σχετικών διεθνών κατευθυντήριων γραμμών, οι οποίες αξιολογούν τους κινδύνους που σχετίζονται με θέματα ασφάλειας των πληροφοριών και τα νομικά ζητήματα προστασίας δεδομένων και δίνουν προτεραιότητα στα ευρήματα, ανάλογα με το επίπεδο κινδύνου.

4. Δημιουργήσει λεπτομερές πλάνο ενεργειών αντιμετώπισης και διαχείρισης των ευρημάτων, έτσι ώστε οι επικεφαλής όλων των επιμέρους κλινικών, μονάδων, τμημάτων να είναι σε θέση να εφαρμόσουν τις απαραίτητές ενέργειες.

5. Παρέχει ένα λεπτομερές data flow map ανά οργανική μονάδα/τμήμα ή ανά κατηγορία προσωπικών δεδομένων με σκοπό την πλήρη συμβατότητα με τις απαιτήσεις του GDPR σχετικά με τα αρχεία των δραστηριοτήτων επεξεργασίας.

6. Πραγματοποιήσει έλεγχο σε όλες τις εμπλεκόμενες εφαρμογές λογισμικού, σε όλα τα αποθηκευτικά μέσα (ψηφιακά, έντυπα, ηχητικά, κ.α.) καθώς και να προτείνει με σαφήνεια τις απαιτούμενες αλλαγές και τροποποιήσεις βάσει του νέου κανονισμού. Η αξιολόγηση θα περιλαμβάνει το σύνολο των συλλεγόμενων προσωπικών δεδομένων, της νομικής βάσης πάνω στην οποία στηρίζεται η συλλογή, της παρεχόμενης συναίνεσης από τον εκάστοτε συμβαλλόμενο των παρεχόμενων πληροφοριών κλπ.

7. Παρέχει λίστα προτάσεων σχετικά με τις αναγκαίες δράσεις αντιμετώπισης (συμπεριλαμβανομένων και των προτεινόμενων τεχνολογικών λύσεων) για κάθε κενό ή έλλειψη που προκύπτει.

8. Καταρτίσει εγχειρίδια και πολιτικές για την εφαρμογή των διατάξεων του Κανονισμού από το προσωπικό του Νοσοκομείου.

9. Καταρτίσει εγχειρίδιο αντιμετώπισης πιθανών κρίσεων λόγω παραβίασης των προσωπικών δεδομένων.

10. Συντάξει πλάνο επιχειρηματικής συνέχειας για την ομαλή λειτουργία του Νοσοκομείου.

11. Πραγματοποιήσει αξιολόγηση όλων των διαφορετικών τύπων συμβάσεων του νοσοκομείου με τρίτους, να εντοπίσει κενά και να προτείνει ενέργειες με σκοπό την προσαρμογή τους στον GDPR.

12. Πραγματοποιήσει αξιολόγηση όλων των πρακτικών που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων και να παρέχει συγκεκριμένες και λεπτομερείς προτάσεις για δράσεις συμμόρφωσης με τον Κανονισμό.

13. Παρέχει ένα λεπτομερές, προτεραιοποιημένο και ολοκληρωμένο πλάνο συμμόρφωσης. Όλες οι προτεινόμενες ενέργειες συμμόρφωσης είναι απαραίτητο να καλύπτουν ολόκληρο τον κύκλο ζωής των προσωπικών δεδομένων (δηλαδή συλλογή, καταγραφή, τροποποίηση/ενημέρωση, αποθήκευση, μεταφορά, διαγραφή/καταστροφή κλπ.) και να έχουν συμφωνηθεί με την ομάδα έργου και τους

επιχειρησιακούς ιδιοκτήτες των δεδομένων του Νοσοκομείου πριν την παράδοση του πλάνου συμμόρφωσης.

14. Τηρεί τις αρχές της εμπιστευτικότητας. Ο ανάδοχος οφείλει να αναλάβει την ευθύνη για τη διασφάλιση της εμπιστευτικότητας των εμπλεκόμενων συμβούλων και τεχνικών, όσον αφορά τη μη διαρροή πληροφοριών του είδους, του βαθμού διεκπεραίωσης της εργασίας καθώς και τις λεπτομέρειες αυτού, σε οποιοδήποτε άτομο ή ομάδα ατόμων.

Λαμβάνοντας υπόψη τα παραπάνω προτείνονται οι ακόλουθες φάσεις υλοποίησης του έργου με τα αντίστοιχα παραδοτέα. Ο ανάδοχος μπορεί να ακολουθήσει οποιαδήποτε οργάνωση για την πρόταση του αρκεί να περιλαμβάνει κατ' ελάχιστον τις υπηρεσίες που αναφέρονται.

Φάσεις του Έργου – Παραδοτέα

Φάση 1: Έναρξη του Έργου - Οργάνωση Δράσεων

1. Πλήρης ενημέρωση της Διοίκησης και των στελεχών του Νοσοκομείου σχετικά με τα άρθρα και τις απαιτήσεις του κανονισμού.
2. Υποβολή προτάσεων οργάνωσης της Ομάδας του Έργου
3. Παρουσίαση του σχεδίου στη Διοίκηση και τα στελέχη του Νοσοκομείου.

Παραδοτέα

1. Πλάνο υλοποίησης έργου (Περιγραφή του Έργου στην οποία περιγράφεται ο τρόπος προσέγγισης και εκτέλεσης του Έργου, συμπεριλαμβανομένης της σύνθεσης της Ομάδας Έργου, των παραδοτέων και του χρονοδιαγράμματος).

Φάση 2 - Χαρτογράφηση Δεδομένων –Data Mapping

Αρχικά απαιτείται από τον ανάδοχο αποτύπωση της υφιστάμενης κατάστασης σε σχέση με τις απαιτήσεις του Κανονισμού. Αυτό δύναται να γίνει με την μορφή συνεντεύξεων ή/και με οποιονδήποτε άλλο τρόπο κρίνεται απαραίτητος, προκειμένου να καθοριστεί ο κύκλος ζωής των δεδομένων προσωπικού χαρακτήρα, και ιδιαίτερα των προσωπικών δεδομένων ειδικής κατηγορίας, σε όλα τα τμήματα του Νοσοκομείου. Παράλληλα θα δημιουργηθούν τα απαραίτητα αρχεία τεκμηρίωσης που θα πρέπει να έχει στην κατοχή του το Νοσοκομείο σε σχέση με τον Κανονισμό.

Η φάση αυτή περιλαμβάνει τουλάχιστον τις ακόλουθες δράσεις:

1. Επισκόπηση των επιχειρησιακών, τεχνικών και λειτουργικών διαδικασιών.
2. Συγκέντρωση των απαιτούμενων πληροφοριών για τη συλλογή και επεξεργασία των προσωπικών δεδομένων, μέσω της διενέργειας συνεντεύξεων με το αρμόδιο προσωπικό όλων των Τμημάτων.
3. Δημιουργία διαγραμμάτων ροής δεδομένων που θα αποτυπώνουν τις φάσεις του κύκλου ζωής των δεδομένων, από τη συλλογή, χρήση, αποθήκευση, μεταφορά μέχρι και την καταστροφή τους.
4. Δημιουργία του αρχείου δραστηριοτήτων και πόρων επεξεργασίας του Νοσοκομείου με έμφαση σε όλες τις κρίσιμες περιοχές επεξεργασίας.
5. Εντοπισμός προσωπικών δεδομένων σε συστήματα με δομημένες και αδόμητες πληροφορίες του Νοσοκομείου.
6. Εντοπισμός των κρίσιμων αποκλίσεων έναντι των απαιτήσεων του GDPR.
7. Μελέτη και επισκόπηση δικτύου

Ιδιαίτερη προσοχή πρέπει να δώσει ο ανάδοχος στην **αποτύπωση** του συνόλου των δραστηριοτήτων επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του Νοσοκομείου. Η αποτύπωση θα πρέπει τουλάχιστον να καλύπτει τις απαιτήσεις του άρθρου 30 και θα περιλαμβάνει κατ' ελάχιστον:

1. Το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου υπαλλήλου επεξεργασίας και του υπεύθυνου προστασίας των δεδομένων.

2. Τον όγκο και την μορφή των πληροφοριών (πλήθος εγγραφών, πλήθος εγγράφων, αριθμού σελίδων κλπ, χαρτί ή ηλεκτρονικό, δομημένο ή αδόμητο).

3. Τους σκοπούς της επεξεργασίας και τις ανάγκες που καλύπτουν.

4. Την κατηγορία των δεδομένων.

5. Την περιγραφή των δεδομένων (π.χ. όνομα, φυσική διεύθυνση, διεύθυνση ηλεκτρονικού ταχυδρομείου, αναγνωριστικό ταυτότητας (ΑΔΤ, ΑΦΜ, ΑΜΚΑ κλπ), ιατρικό ιστορικό, αποτελέσματα και γνωματεύσεις εξετάσεων κ.λπ.).

6. Την κατηγοριοποίηση των προσωπικών στοιχείων ταυτότητας (μη ταυτοποίηση, μερική ταυτοποίηση, ταυτοποίηση, ευαίσθητα προσωπικά δεδομένα, κ.λπ.).

7. Τις κατηγορίες αποδεκτών στους οποίους έχουν διαβιβαστεί ή πρόκειται να γνωστοποιηθούν τα προσωπικά δεδομένα.

8. Τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων.

9. Γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας που αναφέρονται στο άρθρο 32 παράγραφος 1.

10. Υλικό τεκμηρίωσης που βασίζεται η επεξεργασία.

11. Όποια άλλα στοιχεία σχετίζονται με την επεξεργασία δεδομένων

Επισημαίνεται ότι η χαρτογράφηση των δεδομένων αναμένεται να γίνει και μέσω συνεντεύξεων και θα καλύπτει περιοχές όπως δεδομένα σε Φυσικό Αρχείο, Έγχαρτη/Ψηφιακή ή Αναλογική μορφή (πχ. CCTV), εμπλεκόμενες εφαρμογές/εργαλεία και λόγους συλλογής τους από το Νοσοκομείο.

Παραδοτέα:

1. Αναφορές με προσωπικά δεδομένα που εντοπίστηκαν στα συστήματα προς ανάλυση.

2. Data Inventory and Data Flow Mapping που θα καλύπτουν την απαίτηση του GDPR σχετικά με το αρχείο δραστηριοτήτων επεξεργασίας δεδομένων και θα

περιέχουν όλες τις επιπλέον απαραίτητες πληροφορίες, ώστε να απεικονίζεται πλήρως η τρέχουσα κατάσταση ως προς τη διαχείριση προσωπικών δεδομένων και να είναι εφικτός ο εντοπισμός κενών ως προς τις απαιτήσεις του θεσμικού πλαισίου (διαγράμματα ροής δεδομένων προσωπικού χαρακτήρα, με κρίσιμες πληροφορίες).

3. Αρχείο δραστηριοτήτων επεξεργασίας δεδομένων

Φάση 3 - Μελέτη ανάλυσης Ελλείψεων και Αποκλίσεων (Gap Analysis και Maturity Assessment)

Μετά την αποτύπωση των δραστηριοτήτων του Νοσοκομείου σε σχέση με τα δεδομένα προσωπικού χαρακτήρα ο ανάδοχος θα διενεργήσει εκτίμηση και αξιολόγηση της αποτελεσματικότητας των υπαρχόντων τεχνικών και οργανωτικών μέτρων του Νοσοκομείου σε σχέση με τις απαιτήσεις του Κανονισμού, συμπεριλαμβανομένης της ασφάλειας και των κινδύνων της επεξεργασίας. Κατά την αποτίμηση θα πρέπει να καταγραφούν τα πιθανά «κενά» συμμόρφωσης, να προσδιοριστούν και να αξιολογηθούν οι επιπτώσεις τους για το Νοσοκομείο και να τεθούν οι κατάλληλες προτεραιότητες για την αντιμετώπισή τους. Η αποτίμηση θα αφορά τόσο την «επάρκεια» των διαδικασιών καθώς και τον «βαθμό υλοποίησης» αυτών.

Η αποτίμηση της επάρκειας θα αξιολογήσει τις εφαρμοζόμενες πολιτικές ασφαλείας, τις υπάρχουσες διαδικασίες, πρακτικές, και οδηγίες (εγκύκλιοι, νόμοι, κανονισμοί) που επηρεάζουν τη διαχείριση των δεδομένων προσωπικού χαρακτήρα, ως προς την επάρκεια τους σε σχέση με τις απαιτήσεις του κανονισμού ανά άρθρο.

Η αποτίμηση του βαθμού υλοποίησης θα προσδιορίσει τον βαθμό της πραγματικής χρήσης των πολιτικών ασφαλείας και των διαδικασιών σε όλα Τμήματα του Νοσοκομείου.

Ενδεικτικά η φάση αυτή πρέπει να περιλαμβάνει τουλάχιστον τις ακόλουθες δράσεις:

1. Μελέτη υφιστάμενης κατάστασης ως προς τη διαχείριση προσωπικών δεδομένων από άποψη:

- Νομική
- Οργάνωσης, Πολιτικών Και Διαδικασιών
- Ασφάλειας Πληροφοριών
- Τεχνολογική

2. Εντοπισμός των πεδίων μη συμμόρφωσης στις πρακτικές και διαδικασίες που εφαρμόζονται κατά τον χειρισμό των προσωπικών δεδομένων, ως προς:
   - τις απαιτήσεις του GDPR
   - τις απαιτήσεις των οδηγιών, κατευθύνσεων και αποφάσεων της WP29, της ΑΠΔΠΧ και των Ευρωπαϊκών Αρχών Προστασίας Δεδομένων
   - το κανονιστικό πλαίσιο του έργου, συμπεριλαμβανομένων σχετικών δικαστικών αποφάσεων
   - τις απαιτήσεις των διεθνών προτύπων ISO 27001, ISO 27002 για την ασφάλεια των πληροφοριών
3. Μελέτη ως προς τις υφιστάμενες επεξεργασίες δεδομένων (και της διαβαθμίσεώς τους) σε συνδυασμό με τα εμπλεκόμενα συστήματα πληροφορικής του Νοσοκομείου
4. Αναγνώριση των υφιστάμενων αποκλίσεων από τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων ως προς τις επιμέρους περιοχές επεξεργασίας προσωπικών δεδομένων
5. Μελέτη αποκλίσεων της υφιστάμενης κατάστασης του Νοσοκομείου σε σχέση με τις απαιτήσεις του Κανονισμού για κάθε επεξεργασία. Η μελέτη θα πρέπει να περιλαμβάνει τουλάχιστον τις παρακάτω περιοχές:
   - Απαιτήσεις ως προς την υποχρέωση τήρησης αρχείου δραστηριοτήτων
   - Συναίνεση
   - Συλλογή, Χρήση, Αποθήκευση
   - Διατήρηση δεδομένων/Καταστροφή

- Δικαιώματα πρόσβασης, διόρθωσης, αλλαγής, φορητότητας και διαγραφής
- Κοινοποίηση σε Τρίτα Μέρη
- Διαβίβαση σε τρίτες χώρες
- Ασφάλεια επεξεργασίας προσωπικών δεδομένων
- Έλεγχος και παρακολούθηση των οργανωτικών και τεχνολογικών μέτρων
- Πόροι
- Γνωστοποίηση παραβίασης Προσωπικών Δεδομένων σε εποπτική αρχή ή/και στο υποκείμενο των δεδομένων

6. Καταγραφή των σχετικών ευρημάτων σε σχέση με το βαθμό ετοιμότητας συμμόρφωσης του Νοσοκομείου και τις επιμέρους αποκλίσεις που παρουσιάζει σε σχέση με τις ανωτέρω απαιτήσεις.

Παραδοτέα

1. Gap Analysis

Φάση 4 – Διενέργεια Privacy and Data Protection Impact Assessment, Αποτίμηση Επικινδυνότητας και Ανάπτυξη σχεδίου διορθωτικών ενεργειών

Λόγω της φύσης των δεδομένων προσωπικού χαρακτήρα που διατηρούνται στο Νοσοκομείο, ο Κανονισμός επιβάλει τη διενέργεια εκτίμησης αντικτύπου (Data Protection Impact Assessment, DPIA). Η εκτίμηση αντικτύπου που θα διεξάγει ο ανάδοχος θα πρέπει να περιλαμβάνει με βάση το άρθρο 35 παρ. 7 τουλάχιστον:

1. Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει το Νοσοκομείο.
2. Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς.

3. Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (υποκειμένων των δεδομένων).

4. Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον Κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

Ο ανάδοχος βασισμένος στην ανάλυση του βαθμού συμμόρφωσης καθώς και στην εκτίμηση αντικτύπου, θα διεξάγει **αποτίμηση επικινδυνότητας**. Η αποτίμηση θα βασίζεται στις οδηγίες και τη δομή του προτύπου ISO 27005:2011, θα περιλαμβάνει την αποτίμηση της τρέχουσας κατάστασης και την εκτίμηση των κινδύνων για τα δεδομένα προσωπικού χαρακτήρα που διατηρούνται στο Νοσοκομείο, των απειλών και των ευπαθειών των εξεταζόμενων συστημάτων, ηλεκτρονικών ή μη (στα οποία είναι αποθηκευμένα τα προσωπικά δεδομένα). Η αποτίμηση θα γίνει με βάση την επίδραση που θα έχει η διαρροή, αποκάλυψη ή η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή τους, στα φυσικά πρόσωπα που αφορούν και στην ομαλή λειτουργία του Νοσοκομείου.

Πιο συγκεκριμένα, θα προσδιορίζονται οι απειλές οι οποίες σχετίζονται με τα δεδομένα προσωπικού χαρακτήρα και στη συνέχεια θα εκτιμάται το επίπεδο της κάθε απειλής. Αμέσως μετά θα αποτιμάται η έκταση των ευπαθειών που μπορεί να εκμεταλλευτεί η κάθε απειλή.

Μετά την αποτίμηση επικινδυνότητας, η Διοίκηση του Νοσοκομείου, με την βοήθεια του αναδόχου, θα αποφασίσει για την διαχείριση των απειλών των δεδομένων προσωπικού χαρακτήρα, εξετάζοντας λύσεις όπως την Αποδοχή του Επιπέδου Επικινδυνότητας, την Μεταβίβαση του Επιπέδου Επικινδυνότητας, την Αντιμετώπιση του Επιπέδου Επικινδυνότητας και άλλες.

Τέλος, στις περιπτώσεις που επιλεγεί η αντιμετώπιση του επιπέδου επικινδυνότητας, ο ανάδοχος οφείλει να προτείνει κατάλληλα μέτρα και μηχανισμούς ασφαλείας που πρέπει να υιοθετηθούν ώστε το Νοσοκομείο να δύναται να διαχειριστεί τον πιθανό

αντίκτυπο μιας διαρροής, αποκάλυψης ή μη εξουσιοδοτημένης τροποποίησης ή καταστροφής.

Ολοκληρούμενη η φάση αυτή πρέπει να περιλαμβάνει τουλάχιστον τις ακόλουθες δράσεις:

- Διενέργεια Privacy Impact Assessment με βάση τις έγκυρες πρακτικές και μεθοδολογίες, που αναφέρθηκαν ανωτέρω.
- Σύνταξη αναλυτικού και σαφούς σχεδίου στο οποίο θα:
    - συμπεριλαμβάνονται οι προτάσεις βελτίωσης ανά τμήμα και Οργανική Μονάδα του Νοσοκομείου, με σκοπό την αντιμετώπιση των ελλείψεων ή/και αποκλίσεων σε σχέση με τις απαιτήσεις του Κανονισμού και τις απαιτήσεις του ευρύτερου κανονιστικού πλαισίου και των προτύπων, όπως αναλύονται παραπάνω.
    - προσδιορίζονται συγκεκριμένες ενέργειες και εργασίες, ώστε να βελτιωθεί κατά το δυνατόν συντομότερα το επίπεδο συμμόρφωσης.
    - περιλαμβάνονται προτάσεις με σκοπό τη συμμόρφωση με τον GDPR μέσω
        - της τροποποίησης υφιστάμενων διαδικασιών,
        - της τροποποίησης του περιβάλλοντος λειτουργίας των πληροφοριακών συστημάτων,
        - της διατήρησης στο μέλλον ικανοποιητικού επίπεδου συμμόρφωσης,
        - της συστηματικής αύξησης του επιπέδου συμμόρφωσης βάσει χρονοδιαγράμματος που θα προσδιοριστεί σε συνεργασία με το Νοσοκομείο.

Παραδοτέα

1. Privacy Impact Assessment

2. Εκτίμηση αντικτύπου (Data Protection Impact Assessment)

3. Αποτίμηση Επικινδυνότητας (Risk Assessment)

4. Compliance Plan που να συμπεριλαμβάνει προτάσεις αλλαγών για την ικανοποίηση των απαιτήσεων στις διαδικασίες, τα μη ψηφιακά αρχεία και τα Πληροφοριακά Συστήματα του Νοσοκομείου.

Φάση 5 - Σχέδιο δράσης συμμόρφωσης -security policies and handbooks

Μετά την εκτίμηση της υφιστάμενης κατάστασης, την εκτίμηση αντικτύπου και την αποτίμηση επικινδυνότητας, ο ανάδοχος θα αναλάβει να εκπονήσει και να τεκμηριώσει σχέδιο δράσης για συμμόρφωση του Νοσοκομείου με τις απαιτήσεις του Κανονισμού. Το σχέδιο θα περιλαμβάνει το σύνολο των απαιτούμενων Πολιτικών και Διαδικασιών για την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα με βάση τις απαιτήσεις του Κανονισμού. Μεταξύ των άλλων θα επικεντρώνεται στον τρόπο με τον οποίο θα γίνεται η συλλογή, αποθήκευση, επεξεργασία και διαχείριση των δεδομένων προσωπικού χαρακτήρα καθώς και η συναίνεση του υποκειμένου, το δικαίωμα στη διαγραφή (το «δικαίωμα στη λήθη»), η καταγραφή και γνωστοποίηση παραβιάσεων (διαδικασία γνωστοποίησης της παραβίασης δεδομένων & σχέδιο απόκρισης σε περίπτωση συμβάντων) και των πολιτικών και διαδικασιών για ενημερώσεις, επιθεωρήσεις και συνεχή βελτίωση.

Το σχέδιο δράσης θα πρέπει να περιλαμβάνει ανά άρθρο του Κανονισμού όλες τις απαραίτητες πολιτικές και διαδικασίες που απαιτούνται για την συμμόρφωση του Νοσοκομείου με αυτόν.

Ενδεικτικά αναφέρονται:

- Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που πληροί τις νομικές απαιτήσεις και αντιμετωπίζει το λειτουργικό κίνδυνο και τον κίνδυνο βλάβης των ατόμων.
- Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα των εργαζομένων.
- Κώδικας Δεοντολογίας που περιλαμβάνει άρθρα για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα.

- Πολιτική/διαδικασίες για τη συλλογή και τη χρήση προσωπικών δεδομένων ειδικής κατηγορίας.
- Πολιτική/διαδικασίες για τη συλλογή και χρήση των δεδομένων προσωπικού χαρακτήρα παιδιών και ανηλίκων.
- Πολιτική/διαδικασίες για τη διατήρηση της ποιότητας των δεδομένων.
- Πολιτική/διαδικασίες για τη διαγραφή των προσωπικών δεδομένων.
- Πολιτική/διαδικασίες για τον έλεγχο της επεξεργασίας που διεξάγεται συνολικά ή εν μέρει με αυτοματοποιημένα μέσα.
- Πολιτική/διαδικασίες για δευτερεύουσες χρήσεις των δεδομένων προσωπικού χαρακτήρα.
- Πολιτική/διαδικασίες για την απόκτηση έγκυρης συναίνεσης.
- Πολιτική/διαδικασίες για ασφαλή καταστροφή των δεδομένων.
- Πολιτική/διαδικασίες για τη διατήρηση αρχείων.
- Πολιτική/διαδικασίες - όσον αφορά τα δεδομένα προσωπικού χαρακτήρα - για άμεση επικοινωνία, ηλεκτρονικό ταχυδρομείο, κλπ.
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε συμβόλαια συντήρησης και υποστήριξης.
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές πρόσληψης/απασχόλησης.
- Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ιστοσελίδα του Νοσοκομείου και στα μέσα κοινωνικής δικτύωσης.
- Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές υγιεινής και ασφάλειας.
- Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στις πρακτικές παρακολούθησης και αξιολόγησης των εργαζομένων.

- Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πολιτικές / διαδικασίες σχετικά με την πρόσβαση σε λογαριασμούς εταιρικού ηλεκτρονικού ταχυδρομείου των εργαζομένων.
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στη διεξαγωγή εσωτερικών επιθεωρήσεων.
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα για την αντιμετώπιση καταγγελιών.
- Διαδικασίες ανταπόκρισης σε αιτήματα πρόσβασης σε προσωπικά δεδομένα.
- Διαδικασίες ανταπόκρισης σε αιτήματα διόρθωσης δεδομένων προσωπικού χαρακτήρα.
- Διαδικασίες ανταπόκρισης σε αιτήματα για εξαίρεση, περιορισμό της επεξεργασίας ή αντιρρήσεις στην επεξεργασία.
- Διαδικασίες ανταπόκρισης στα αιτήματα για πληροφορίες.
- Διαδικασίες ανταπόκρισης στα αιτήματα φορητότητας δεδομένων.
- Διαδικασίες (οργανωτικές και τεχνικές) ανταπόκρισης σε αιτήματα για διαγραφή δεδομένων.
- Διαδικασίες καταγραφής παραπόνων σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.
- Πολιτική/Διαδικασίες διαχείρισης των παραβιάσεων της ασφάλειας των προσωπικών δεδομένων ή της διαρροής αυτών.
- Σχέδιο αντιμετώπισης περιστατικών παραβίασης, διατήρηση αρχείου καταγραφής με στοιχεία όπως η φύση της παραβίασης, ο κίνδυνος, η προέλευση.
- Διαδικασίες κοινοποίησης της παραβίασης (στα ενδιαφερόμενα άτομα) και υποβολή αναφορών (σε ρυθμιστικές αρχές, πιστωτικές υπηρεσίες, κ.λπ.).
- Διαδικασία συνεχούς παρακολούθησης και ενημέρωσης για νέες απαιτήσεις συμμόρφωσης, προσδοκίες και βέλτιστες πρακτικές.

Επίσης θα πρέπει να αναπτυχθούν όλες οι απαραίτητες πολιτικές και διαδικασίες σε σχέση με τους συνεργάτες (προμηθευτές / συμβούλους / εταιρίες υποστήριξης / Δημόσιους φορείς, κλπ) οι οποίες θα προστεθούν στα υπάρχοντα ή νέα συμβόλαια. Ενδεικτικά θα περιλαμβάνονται:

- Απαιτήσεις από τους συνεργάτες για την προστασία των δεδομένων προσωπικού χαρακτήρα κατά την εκτέλεση συμβάσεων ή συμφωνιών.
- Όροι για δέουσα επιμέλεια σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα.
- Δυνατότητα αξιολόγησης του κινδύνου που προέρχεται από τους συνεργάτες (right to audit).

Το σχέδιο δράσης θα περιλαμβάνει επίσης:

- Κατάρτιση εγχειριδίων και πολιτικών για την εφαρμογή των διατάξεων του Κανονισμού από το προσωπικό του Νοσοκομείου.
- Κατάρτιση εγχειριδίου Αντιμετώπισης πιθανών κρίσεων λόγω παραβίασης των προσωπικών δεδομένων.
- Πλάνο επιχειρηματικής συνέχειας για την ομαλή λειτουργία του Νοσοκομείου.

Οι παραπάνω ενέργειες του σχεδίου δράσης είναι ενδεικτικές. Το σύνολο των απαιτούμενων ενεργειών για συμμόρφωση του Νοσοκομείου με τον κανονισμό θα καθοριστούν με βάση τα αποτελέσματα των προηγούμενων φάσεων.

Παραδοτέα

1. Εκθέσεις, ευρήματα και προτεινόμενες διορθωτικές ενέργειες για κάθε επιθεωρούμενο τμήμα του Νοσοκομείου μετά από το Internal Audit.
2. Σχέδιο Δράσης Συμμόρφωσης με τις απαραίτητες πολιτικές και διαδικασίες, ανά άρθρο του Κανονισμού και παρουσίαση του σχεδίου δράσης.
3. Πρόγραμμα και σχέδιο εσωτερικών επιθεωρήσεων
4. Σχέδιο Δράσεων ευαισθητοποίησης

5. Σχέδιο Δράσεων εκπαίδευσης και επιμόρφωσης
6. Εκπαιδευτικό και ενημερωτικό υλικό
7. Κατάρτιση εγχειριδίου προστασίας δεδομένων
8. Κώδικας Δεοντολογίας

Φάση 6 – Υλοποίηση έργου

Ο ανάδοχος, μετά την έγκριση από την Διοίκηση, έχει υποχρέωση να υλοποιήσει το Σχέδιο Δράσης Συμμόρφωσης. Οι υποχρεώσεις του αναδόχου αφορούν τουλάχιστον:

- Την υλοποίηση όλων των μέτρων/ενεργειών/διαδικασιών οι οποίες δεν απαιτούν την προμήθεια ή τροποποίηση εξοπλισμού/προγραμμάτων.
- Την σύνταξη όλων των Πολιτικών/Διαδικασιών που απαιτούνται για την εναρμόνιση του Νοσοκομείου με τον Κανονισμό.
- Την παροχή υπηρεσιών συμβούλου στην υλοποίηση των μέτρων/ενεργειών που απαιτούν την προμήθεια ή τροποποίηση εξοπλισμού/προγραμμάτων.
- Την εκπαίδευση του προσωπικού του Νοσοκομείου που εμπλέκεται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Ο ανάδοχος είναι υπεύθυνος για την υλοποίηση του σχεδίου δράσης.

Η σωστή εκπαίδευση του προσωπικού του Νοσοκομείου είναι κρίσιμη για την διαφύλαξη της ασφάλειας των δεδομένων προσωπικού χαρακτήρα. Για τον λόγο αυτόν, το προσωπικό του Νοσοκομείου θα πρέπει να εκπαιδευτεί κατάλληλα από τον ανάδοχο ώστε:

- Να είναι ενήμερο για τον Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), τις απαιτήσεις του και την υποχρέωση του Νοσοκομείου να συμμορφώνεται με αυτόν.
- Να είναι γνώστης των Πολιτικών Προστασίας των δεδομένων προσωπικού χαρακτήρα καθώς και των διαδικασιών εφαρμογής τους και να τις αποδέχεται.

– Να καταλαβαίνει πλήρως το ρόλο και τις ευθύνες που του έχουν ανατεθεί σχετικά με τη συμμόρφωση με τον Κανονισμό.

– Να γνωρίζει λεπτομερώς τις διαδικασίες αντιμετώπισης συμβάντων αλλά και τις υπόλοιπες κρίσιμες διαδικασίες.

Λόγω του μεγέθους του Νοσοκομείου οι εκπαιδευτικές ανάγκες είναι σύνθετες και πρέπει να αντιμετωπιστούν με πολλούς τρόπους. Ο ανάδοχος θα πρέπει να καλύπτει τουλάχιστον τις εξής εκπαιδευτικές διαδικασίες:

– Εκπαίδευση κατά την διάρκεια της εργασίας (on-the-job-training)

– Μαζική εκπαίδευση.

– Εκπαιδευτικό και ενημερωτικό υλικό.

Παραδοτέα

1. Τεκμηρίωση της υλοποίησης από τον ανάδοχο του Σχεδίου Δράσης.

2. Διαδικασίες και πολιτικές συμμόρφωσης με τον Κανονισμό

Φάση 7 - Επιθεώρηση Συμμόρφωσης - Παρουσίαση Αποτελεσμάτων Επιθεώρησης

Η διαδικασία συμμόρφωσης του Νοσοκομείου με τον Κανονισμό θα πρέπει να ολοκληρωθεί με την τελική επιθεώρηση συμμόρφωσης από τον ανάδοχο για τη διατήρηση της συμμόρφωσης και την τήρηση των προβλεπόμενων αρχείων που μπορούν να χρησιμοποιηθούν τόσο για εσωτερική όσο και για εξωτερική αναφορά.

Κατά τη φάση της επιθεώρησης συμμόρφωσης από τον ανάδοχο θα επιθεωρηθούν οι εργαζόμενοι, οι χώροι εργασίας τους, τα σημεία αποθήκευσης των προσωπικών δεδομένων - έγγραφων και ηλεκτρονικών-, η πρόσβαση σε αυτά, οι χρησιμοποιούμενες πολιτικές και διαδικασίες καθώς επίσης και οι συμφωνίες εμπιστευτικότητας που έχουν υπογράφει, ώστε να επιβεβαιωθεί η διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα και των απαιτήσεων του Κανονισμού.

Επιπλέον, θα επιθεωρηθούν ο τρόπος επικοινωνίας με τους συνεργάτες, το είδος της πληροφορίας που ανταλλάσσεται (στην περίπτωση που ανταλλάσσονται προσωπικά δεδομένα) και η αποθήκευσή της. Σημαντικό στοιχείο ελέγχου είναι οι Συμφωνίες Εμπιστευτικότητας και τα Συμβόλαια Συντήρησης/Υποστήριξης που έχουν υπογραφεί με τους συνεργάτες, καθώς και το είδος της εκπαίδευσης / ενημέρωσης που έχουν λάβει, όσον αφορά την προστασία των προσωπικών δεδομένων.

Μετά την ολοκλήρωση της επιθεώρησης συμμόρφωσης, ο ανάδοχος θα πρέπει να επικαιροποιήσει:

- Αρχεία Τεκμηρίωσης
- Αρχεία Δραστηριοτήτων Επεξεργασίας
- Ανάλυση του επιπέδου συμμόρφωσης του Νοσοκομείου, ανά άρθρο του Κανονισμού.
- Εκτίμηση αντικτύπου (Data Protection Impact Assessment)
- Αποτίμηση Επικινδυνότητας (Risk Assessment)
- Σχέδιο Δράσης Συμμόρφωσης με τα συμπληρωματικά μέτρα και διαδικασίες, ανά άρθρο του Κανονισμού που θα πρέπει να υλοποιηθούν
- Ο ανάδοχος αναλαμβάνει να εκτελέσει όποιο συμπληρωματικό μέτρο / ενέργεια προκύψει και στη συνέχεια να συντάξει τελική έκθεση με τα αποτελέσματα του εσωτερικού ελέγχου.

Ο ανάδοχος θα παρουσιάσει στην Διοίκηση του Νοσοκομείου τα αποτελέσματα της επιθεώρησης συμμόρφωσης καθώς και του επικαιροποιημένου Data Protection Impact Assessment και Risk Assessment.

Επίσης, θα αναλυθούν οι μεγαλύτεροι κίνδυνοι που αντιμετωπίζει το Νοσοκομείο όσον αφορά τα δεδομένα προσωπικού χαρακτήρα και ιδιαίτερα όσο αφορά τα προσωπικά δεδομένα ειδικής κατηγορίας.

Παραδοτέα

1. Επικαιροποιημένο Αρχείο Τεκμηρίωσης
2. Επικαιροποιημένο Αρχείο Δραστηριοτήτων Επεξεργασίας
3. Επικαιροποιημένη Ανάλυση του επιπέδου συμμόρφωσης του Νοσοκομείου, ανά άρθρο του Κανονισμού.
4. Επικαιροποιημένη Εκτίμηση Αντικτύπου (Data Protection Impact Assessment)
5. Επικαιροποιημένη Αποτίμηση Επικινδυνότητας (Risk Assessment)
6. Σχέδιο Δράσης Συμμόρφωσης με τα συμπληρωματικά μέτρα και διαδικασίες, ανά άρθρο του Κανονισμού
7. Επικαιροποιημένη Πολιτική Ασφαλείας (Security Policy) του Νοσοκομείου.

ΔΙΑΡΚΕΙΑ ΕΚΤΕΛΕΣΗΣ ΤΟΥ ΕΡΓΟΥ Α

Το έργο θα πρέπει να έχει ολοκληρωθεί σε δώδεκα (12) μήνες από την υπογραφή της σύμβασης.

Β. ΥΠΗΡΕΣΙΕΣ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPO) ΤΟΥ ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ - ΟΦΘΑΛΜΙΑΤΡΕΙΟ ΑΘΗΝΩΝ – ΠΟΛΥΚΛΙΝΙΚΗ», ΟΡΓΑΝΙΚΗ ΜΟΝΑΔΑ ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ».

Κατά την διάρκεια της διαδικασίας συμμόρφωσης του Νοσοκομείου με τον Ευρωπαϊκό Κανονισμό Προστασίας Δεδομένων (GDPR), έργο που θα πρέπει να παραδοθεί σε δώδεκα (12) μήνες από την υπογραφή της σύμβασης, και **για ένα έτος** μετά την ολοκλήρωση του ως άνω έργου ο Ανάδοχος θα παρέχει στο Νοσοκομείο κατάλληλα καταρτισμένο και πιστοποιημένο άτομο προκειμένου να αναλάβει τα καθήκοντα του Υπεύθυνου Προστασίας Δεδομένων (DPO).

Ο DPO θα παρακολουθεί την εφαρμογή των Πολιτικών/Διαδικασιών Προστασίας Προσωπικών Δεδομένων που έχουν αναπτυχθεί για την συμμόρφωση του Νοσοκομείου με τον Κανονισμό. Επιπλέον θα αναθεωρεί και θα βελτιώνει τις Πολιτικές / Διαδικασίες όπου κρίνει απαραίτητο. Επίσης θα επικαιροποιεί τις εκτιμήσεις αντίκτυπου (DPIA) και θα δημιουργεί καινούριες για επεξεργασίες υψηλού ρίσκου. Ακόμα θα αναλαμβάνει την ενημέρωση του προσωπικού καθώς και τις εσωτερικές επιθεωρήσεις, με σκοπό την επίτευξη του βέλτιστου επιπέδου συμμόρφωσης.

Ο DPO διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και των εκτελούντων την επεξεργασία προς τις διατάξεις του GDPR και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός). Καταρχήν δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση προς τον GDPR, έχει όμως βέβαια την ευθύνη καθοδήγησης του φορέα προς την απαιτούμενη συμμόρφωση προς τον GDPR.

Αναλυτικά τα καθήκοντα του DPO είναι τα ακόλουθα:

• Να ενημερώνει και να συμβουλεύει τον οργανισμό και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον GDPR και άλλες διατάξεις περί προστασίας δεδομένων.

• Να παρακολουθεί την εσωτερική συμμόρφωση με τον GDPR και άλλες διατάξεις περί προστασίας δεδομένων (π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).

• Να παρέχει συμβουλές για την εκτίμηση αντικτύπου και να παρακολουθεί την υλοποίησή της.

• Να είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, ασθενείς, κ.λπ.).

• Να συνεργάζεται με την εποπτική αρχή και να ενεργεί ως σημείο επικοινωνίας με την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της διαβούλευσης που αναφέρεται στο άρθρο 36 του GDPR.

• Να συμμετέχει σε όλα τα ζητήματα σχετικά με την προστασία προσωπικών δεδομένων (π.χ. παρουσία σε συσκέψεις ανώτερων και μεσαίων στελεχών της διοίκησης ή αντίστοιχα άλλων Φορέων και κατά τη λήψη αποφάσεων, καταγραφή λόγων διαφωνίας με τις συμβουλές του, έγκαιρη διαβίβαση πληροφοριών για παροχή γνώμης, άμεση λήψη γνώμης σε περίπτωση περιστατικού παραβίασης).

• Κατά την εκτέλεση των καθηκόντων του, λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

• Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του εργοδότη, ενώ παράλληλα δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του.

• Είναι σε άμεση συνεργασία με το Γραφείο Υπευθύνου Προστασίας Δεδομένων του Υπουργείου Υγείας για την ενίσχυση των δράσεων προστασίας δεδομένων του Υπουργείου και την εφαρμογή τους στο σύνολο των εποπτευόμενων φορέων με ομοιογενή και εύρυθμο τρόπο.

Η Διοίκηση του Φορέα φροντίζει αντίστοιχα ώστε ο DPO :

• Να έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας

• Να εκπληρώνει τα καθήκοντά του με ανεξάρτητο τρόπο (δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του) και δεν υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του.

ΔΙΑΡΚΕΙΑ ΠΑΡΟΧΗΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ DPO

Κατά την διάρκεια και για ένα έτος μετά την ολοκλήρωση της διαδικασίας συμμόρφωσης του Νοσοκομείου με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), με δυνατότητα παράτασης για ακόμη ένα έτος με τη σύμφωνη γνώμη των συμβαλλομένων.

Γ) ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΠΕΙΛΩΝ 24Χ7Χ365 ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΧΡΟΝΟ

Παροχή υπηρεσίας διαχείρισης απειλών 24x7x365 σε πραγματικό χρόνο από εξειδικευμένο Επιχειρησιακό Κέντρο Ασφάλειας (Security Operation Center) του Αναδόχου η οποία περιλαμβάνει:

- Ετήσια περιμετρική παρακολούθηση και διαχείριση περιστατικών παραβίασης σε πραγματικό χρόνο 24x7 με σκοπό τον εντοπισμό και την αναφορά των περιστατικών παραβίασης των προσωπικών δεδομένων στο Νοσοκομείο.
- Δημιουργία προσαρμοσμένων σεναρίων επίθεσης στα πληροφοριακά συστήματα του Νοσοκομείου βάση των οποίων θα εντοπίζονται τα περιστατικά παραβίασης από το Διαδίκτυο.
- Κάθε κρίσιμο περιστατικό θα πρέπει να αναφέρεται εντός 15 λεπτών.
- Ενημέρωση για κάθε Περιστατικό Ασφαλείας μέσω e-mail, SMS, τηλεφωνική κλήση. Για κάθε περιστατικό θα πρέπει τουλάχιστον να αναφέρεται η ώρα και ημερομηνία, η κρισιμότητα, οι ενέργειες εξάλειψης.

Παραδοτέα

- Μηνιαία Αναφορά Περιστατικών Ασφαλείας

ΠΡΟΫΠΟΘΕΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ

Ο υποψήφιος Ανάδοχος θα πρέπει να:

- υλοποιεί ή να έχει υλοποιήσει αντίστοιχης έκτασης και πολυπλοκότητας έργα GDPR σε ανάλογου μεγέθους και δραστηριότητας με το ΓΝΑ «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ» Δημόσια ή Ιδιωτικά Νοσοκομεία (τουλάχιστον 2 έργα) και σε άλλους Οργανισμούς Παροχής υπηρεσιών Υγείας ή άλλους Δημόσιους & Ιδιωτικούς οργανισμούς (τουλάχιστον 3 έργα)
- έχει εμπειρία στην παροχή συμβουλευτικών υπηρεσιών στον τομέα της ασφάλειας πληροφοριών.
- έχει και να διαχειρίζεται Επιχειρησιακό Κέντρο Ασφάλειας (Security Operation Center) με τουλάχιστον ένα (1) συναφές έργο στον Τομέα της Υγείας.
- παρέχει υπηρεσίες DPO σε οργανισμούς/εταιρίες του Τομέα Υγείας.
- Διαθέτει ομάδα έργου η οποία θα αποτελείται από τουλάχιστον έναν:
  - Εξειδικευμένο νομικό με γνώση και εμπειρία των πρακτικών περί Προστασίας και Διαχείρισης Προσωπικών Δεδομένων στο πλαίσιο υλοποίησης της συμμόρφωσης. Να αποτελεί ή να έχει αποτελέσει μέλος της ομάδας έργου σε δύο (2) τουλάχιστον παρόμοια έργα.
  - Εξειδικευμένο επιστήμονα Πληροφορικής με γνώση και εμπειρία της ασφαλούς διαχείρισης δεδομένων μέσω πληροφοριακών συστημάτων. Να αποτελεί ή να έχει αποτελέσει μέλος της ομάδας έργου σε δυο (2) τουλάχιστον παρόμοια έργα.

Ένα μέλος της ομάδας έργου, που θα αναλάβει και τον ρόλο του DPO κατά την διάρκεια και για ένα έτος μετά την ολοκλήρωση της διαδικασίας συμμόρφωσης του Νοσοκομείου με τον GDPR, πρέπει να κατέχει πιστοποίηση ή βεβαίωση παρακολούθησης προγράμματος κατάρτισης DPO και να είναι ορισμένος ως DPO σε τουλάχιστον έναν οργανισμό του Τομέα Υγείας. Ένα μέλος της ομάδας θα πρέπει να είναι επιθεωρητής προτύπου διαχείρισης της ασφάλειας των πληροφοριών κατά ISO 27001 ή άλλο διεθνές πρότυπο.

Η εμπειρία και η υλοποίηση των έργων από τον Ανάδοχο θα πρέπει να τεκμηριώνεται με Βεβαίωση από τον πελάτη, ή αντίστοιχη Σύμβαση Έργου.

Ο υποψήφιος Ανάδοχος θα πρέπει να δηλώσει και να διαθέτει τα μέσα διασφάλισης ποιότητας και ασφάλειας των παρεχόμενων υπηρεσιών:

- Να δηλώσει και να διαθέτει σύστημα διαχείρισης ποιότητας και πιστοποίηση κατά ISO 9001:2015, με πεδίο εφαρμογής την παροχή συμβουλευτικών υπηρεσιών και εκπαίδευσης, την παροχή υπηρεσιών συμμόρφωσης με τον Κανονισμό GDPR και την παροχή υπηρεσιών Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO).
- Να δηλώσει και να διαθέτει σύστημα διαχείρισης ασφάλειας πληροφοριών και πιστοποίηση κατά ISO 27001:2013, με πεδίο εφαρμογής την παροχή συμβουλευτικών υπηρεσιών και εκπαίδευσης, την παροχή υπηρεσιών συμμόρφωσης με τον Κανονισμό GDPR και την παροχή υπηρεσιών Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO).
- Να δηλώσει και να διαθέτει σύστημα διαχείρισης επιχειρησιακής συνέχειας και πιστοποίηση κατά ISO 22301:2012, με πεδίο εφαρμογής την παροχή συμβουλευτικών υπηρεσιών και εκπαίδευσης, την παροχή υπηρεσιών συμμόρφωσης με τον Κανονισμό GDPR και την παροχή υπηρεσιών Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO).

Αθήνα, 15-7-2019

Η επιτροπή

ΖΑΓΓΑΝΑ ΠΕΤΡΟΥΛΑ

ΜΠΑΡΜΠΑΡΟΥΣΗ ΜΑΡΙΑ

ΠΑΠΑΙΩΑΝΝΟΥ ΑΝΑΣΤΑΣΙΟΣ