ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
4Η ΥΓΕΙΟΝΟΜΙΚΗ ΠΕΡΙΦΕΡΕΙΑ ΜΑΚΕΔΟΝΙΑΣ ΚΑΙ ΘΡΑΚΗΣ
ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
«ΙΠΠΟΚΡΑΤΕΙΟ»

*Κωνσταντινουπόλεως 49, 546 42 Θεσσαλονίκη*

Υποδιεύθυνση Οικονομικού
Τμήμα Προμηθειών
Πληρ.: Μ. Αργύρη, Κ. Δήμου
☎: 2313 312232, email:promkt@ippokratio.gr

Θεσσαλονίκη, 28 Απριλίου 2022

**ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ**

**ΥΠ΄ΑΡΙΘΜ. 71 /28-04-2022**
**ΓΙΑ ΤΗΝ ΑΝΑΘΕΣΗ ΤΩΝ ΥΠΗΡΕΣΙΩΝ DPO ΣΤΟ ΠΛΑΙΣΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (CPV: 72322000-8) ΓΙΑ ΧΡΟΝΙΚΟ ΔΙΑΣΤΗΜΑ ΕΝΟΣ (1) ΕΤΟΥΣ ΜΕ ΔΙΚΑΙΩΜΑ ΠΡΟΑΙΡΕΣΗΣ ΓΙΑ ΕΝΑ (1) ΕΠΙΠΛΕΟΝ ΕΤΟΣ , ΜΕ ΚΡΙΤΗΡΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΝ ΠΛΕΟΝ ΣΥΜΦΕΡΟΥΣΑ ΑΠΟ ΟΙΚΟΝΟΜΙΚΗ ΑΠΟΨΗ ΠΡΟΣΦΟΡΑ ΒΑΣΕΙ ΤΙΜΗΣ (ΧΑΜΗΛΟΤΕΡΗ ΤΙΜΗ), ΣΥΝΟΛΙΚΗΣ ΠΡΟΫΠΟΛΟΓΙΖΟΜΕΝΗΣ ΔΑΠΑΝΗΣ 30.000,00€ ΧΩΡΙΣ ΦΠΑ (15.000 € ΧΩΡΙΣ ΦΠΑ ΚΑΙ 18.600,00 € ΜΕ Φ.Π.Α. 24% ΓΙΑ ΕΝΑ (1) ΕΤΟΣ), Η ΟΠΟΙΑ ΜΕ ΦΠΑ 24% ΔΙΑΜΟΡΦΩΝΕΤΑΙ ΣΕ 37.200,00€**

Το Γ.Ν.Θ. ΙΠΠΟΚΡΑΤΕΙΟ, σε συνέχεια :

1. Της υπ΄αριθ. Γ4β/Γ.Π.οικ. 2764/16-1-2020 Υπουργική Απόφαση (ΦΕΚ 65/31-1-2020, τ. ΥΟΔΔ) περί διορισμού του Διοικητή στο Γενικό Νοσοκομείο Θεσ/νίκης «ΙΠΠΟΚΡΑΤΕΙΟ», αρμοδιότητας 4ης Υ.ΠΕ. Μακεδονίας και Θράκης, όπως διορθώθηκε με το ΦΕΚ 108/τ.ΥΟΔΔ/14-02-2020.
2. Της απόφασης του Διοικητικού Συμβουλίου του Νοσοκομείου κατά την 4η/23-2-2022 συνεδρίαση του (Θέμα έκτακτο 10ο) (ΑΔΑ: 6ΡΙ3469067-Γ6Λ), σχετικά με την διενέργεια διαγωνιστικής διαδικασίας για την ανάθεση των υπηρεσιών DPO στο πλαίσιο εφαρμογής του Γενικού Κανονισμού Προστασίας Προσωπικών δεδομένων (CPV: 72322000-8), για χρονικό διάστημα ενός (1) έτους με δικαίωμα προαίρεσης για ένα (1) επιπλέον έτος συνολικής προϋπολογιζόμενης δαπάνης 30.000,00 € χωρίς Φ.Π.Α. η οποία με Φ.Π.Α. 24% διαμορφώνεται σε 37.200,00 € (15.000,00 € χωρίς Φ.Π.Α. και 18.600,00 € με Φ.Π.Α. 24% για ένα έτος), σύμφωνα με τις διατάξεις του άρθρου 118, του Ν. 4412/2016 όπως τροποποιήθηκε και ισχύει, με τις τεχνικές προδιαγραφές όπως αυτές κατατέθηκαν με το υπ΄ αριθμ. πρωτ. 26666/15.6.2021 έγγραφο της Επιτροπής σύνταξης τεχνικών προδιαγραφών και εγκρίθηκαν με την απόφαση που έλαβε το Διοικητικό Συμβούλιο κατά την 20η /7.7.2021 (ΑΔΑ:ΩΞΣΚ469067-0ΗΞ) συνεδρίασή του (θέμα έκτακτο 3ο).
3. Των διατάξεις του Ν. 4412/2016 και του ΠΔ 80/2016 όπως τροποποιήθηκαν και ισχύουν.
4. Την υπ' αριθ. 2130/28.4.2022 απόφαση ανάληψης δαπάνης (ΑΔΑ: 6ΖΛΚ469067-ΜΒΞ) στον ΚΑΕ 0439.01.

**ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ**

**ΥΠ΄ΑΡΙΘΜ. 71/28-04-2022**

**ΓΙΑ ΤΗΝ ΑΝΑΘΕΣΗ ΤΩΝ ΥΠΗΡΕΣΙΩΝ DPO ΣΤΟ ΠΛΑΙΣΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (CPV: 72322000-8) ΓΙΑ ΧΡΟΝΙΚΟ ΔΙΑΣΤΗΜΑ ΕΝΟΣ (1) ΕΤΟΥΣ ΜΕ ΔΙΚΑΙΩΜΑ ΠΡΟΑΙΡΕΣΗΣ ΓΙΑ ΕΝΑ (1) ΕΠΙΠΛΕΟΝ ΕΤΟΣ , ΣΥΝΟΛΙΚΗΣ ΠΡΟΫΠΟΛΟΓΙΖΟΜΕΝΗΣ ΔΑΠΑΝΗΣ 30.000,00€ ΧΩΡΙΣ ΦΠΑ , Η ΟΠΟΙΑ ΜΕ ΦΠΑ 24% ΔΙΑΜΟΡΦΩΝΕΤΑΙ ΣΕ 37.200,00€**

**Π ρ ο κ η ρ ύ σ ε ι**

Διαγωνιστική διαδικασία με Πρόσκληση Εκδήλωσης Ενδιαφέροντος – Συλλογή Προσφορών**,** για την ανάθεση υπηρεσιών DPO στο πλαίσιο εφαρμογής του Γενικού Κανονισμού Προστασίας Προσωπικών δεδομένων (CPV: 72322000-8), για χρονικό διάστημα ενός (1) έτους με δικαίωμα προαίρεσης για ένα (1) επιπλέον έτος συνολικής προϋπολογιζόμενης δαπάνης 30.000,00 € χωρίς Φ.Π.Α. η οποία με Φ.Π.Α. 24% διαμορφώνεται σε 37.200,00 € (15.000 € χωρίς Φ.Π.Α. και 18.600,00 € με Φ.Π.Α. 24% για ένα έτος) , με κριτήριο κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει τιμής (χαμηλότερη τιμή).

Προϋπολογιζόμενη δαπάνη: 30.000,00€ χωρίς Φ.Π.Α και 37.200,00€ με ΦΠΑ 24% για δύο (2) έτη.

Η πρόσκληση εκδήλωσης ενδιαφέροντος θα είναι αναρτημένη στο ΚΗΜΔΗΣ και στην ιστοσελίδα του Νοσοκομείου μας .

Πληροφορίες θα δίνονται όλες τις εργάσιμες ημέρες από 08:00πμ έως 14:00μμ από το Τμήμα Προμηθειών του Νοσοκομείου, τηλ. 2313312232, Αρμόδιος υπάλληλος Αργύρη Μαρία.

Προς το σκοπό αυτό, απευθύνει ανοικτή πρόσκληση προς κάθε Οικονομικό Φορέα, που ενδιαφέρεται να υποβάλει την προσφορά του, σύμφωνα με τους παρακάτω όρους :

| | |
|---|---|
| **ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΒΑΣΗΣ:** | ΥΠΗΡΕΣΙΕΣ DPO ΣΤΟ ΠΛΑΙΣΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (CPV: 72322000-8**)** |
| **Κατηγορία CPV** | 72322000-8 ΥΠΗΡΕΣΙΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΔΕΔΟΜΕΝΩΝ |
| **ΔΙΑΡΚΕΙΑ ΣΥΜΒΑΣΗΣ** | Ένα (1) έτος με δικαίωμα προαίρεσης για ένα (1) επιπλέον έτος |
| **ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ:** | 30.000,00€ (15.000,00€ ετησίως) χωρίς Φ.Π.Α και 37.200,00€ (18.600,00€ ετησίως ) με ΦΠΑ 24% για δύο (2) έτη στον ΚΑΕ 0439 |
| **ΤΡΟΠΟΣ ΑΠΟΣΤΟΛΗΣ ΤΩΝ ΠΡΟΣΦΟΡΩΝ:** | *Σε **κλειστό φάκελο,** στον οποίο θα αναγράφονται:*<br>*Ο τίτλος **«ΠΡΟΣΦΟΡΑ ΓΙΑ ΤΗ ΣΥΜΜΕΤΟΧΗ ΣΤΗΝ ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ ΥΠ' ΑΡΙΘΜ.** **71/2022 ΥΠΗΡΕΣΙΩΝ DPO ΣΤΟ ΠΛΑΙΣΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (CPV: 72322000-8) ΓΙΑ ΧΡΟΝΙΚΟ ΔΙΑΣΤΗΜΑ ΕΝΟΣ (1) ΕΤΟΥΣ ΜΕ ΔΙΚΑΙΩΜΑ ΠΡΟΑΙΡΕΣΗΣ ΓΙΑ ΕΝΑ (1) ΕΠΙΠΛΕΟΝ ΕΤΟΣ, ΣΥΝΟΛΙΚΗΣ ΠΡΟΫΠΟΛΟΓΙΖΟΜΕΝΗΣ ΔΑΠΑΝΗΣ 30.000,00€ ΧΩΡΙΣ ΦΠΑ (15.000 € ΧΩΡΙΣ ΦΠΑ ΚΑΙ 18.600,00 € ΜΕ Φ.Π.Α. 24% ΓΙΑ ΕΝΑ (1) ΕΤΟΣ), Η ΟΠΟΙΑ ΜΕ ΦΠΑ 24% ΔΙΑΜΟΡΦΩΝΕΤΑΙ ΣΕ 37.200,00€.**<br>➢ *Τα στοιχεία της εταιρείας*<br>➢ *Η διευκρίνιση: **«ΝΑ ΜΗΝ ΑΝΟΙΧΘΕΙ ΑΠΟ ΤΗΝ ΤΑΧΥΔΡΟΜΙΚΗ ΥΠΗΡΕΣΙΑ Ή ΤΗ ΓΡΑΜΜΑΤΕΙΑ»***<br>*Ο φάκελος να κατατεθεί στο Γραφείο Προμηθειών του Νοσοκομείου, επί της οδού Κωνσταντινουπόλεως 49, ΤΚ 546 42 Θεσσαλονίκη. Με την παράδοση* |

| | |
|---|---|
| | *του φακέλου ο παραδίδων την προσφορά θα παραλαμβάνει από το Γραφείο Προμηθειών απόδειξη παραλαβής της προσφοράς στην οποία θα αναγράφονται τα στοιχεία του Οικονομικού Φορέα, η ημερομηνία και η ώρα παραλαβής της προσφοράς και θα υπογράφεται από τον αρμόδιο υπάλληλο του Νοσοκομείου που παραλαμβάνει την προσφορά και τον παραδίδων αυτή.* |
| **ΧΡΟΝΟΣ ΥΠΟΒΟΛΗΣ ΤΩΝ ΠΡΟΣΦΟΡΩΝ:** | *Η διαδικασία κατάθεσης προσφορών ξεκινά με την ανάρτηση της παρούσας πρόσκλησης.*<br>*Όσοι επιθυμούν να λάβουν μέρος στην Πρόσκληση πρέπει να καταθέσουν έγγραφη σφραγισμένη προσφορά **μέχρι την 3η Μαΐου 2022 ημέρα Τρίτη και ώρα 14.00΄** στο Γραφείο Προμηθειών του Νοσοκομείου.*<br>*Προσφορές που τυχόν υποβληθούν εκπρόθεσμα δεν θα γίνουν δεκτές.*<br>***Η προθεσμία υποβολής των προσφορών τηρείται απαρέγκλιτα**.* |
| **ΠΕΡΙΕΧΟΜΕΝΟ ΠΡΟΣΦΟΡΑΣ:** | *Ο φάκελος της προσφοράς θα περιλαμβάνει:*<br>– *Την **ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ εις διπλούν με** τα ζητούμενα στοιχεία που πρέπει να είναι σύμφωνα με τις απαιτήσεις – υποχρεώσεις του Παραρτήματος Ι, ΙΙ και*<br>– *Την **ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ, εις διπλούν,** δηλαδή τα οικονομικά στοιχεία της προσφοράς, ως εξής:*<br>➢ *Τιμή κόστους της προαναφερόμενης υπηρεσίας.*<br>➢ *Οι τιμές των προσφορών θα εκφράζονται σε Ευρώ.*<br>➢ *Στις τιμές θα περιλαμβάνονται οι τυχόν υπέρ τρίτων κρατήσεις, ως και κάθε άλλη επιβάρυνση, εκτός από τον ΦΠΑ.*<br>➢ *Σε ιδιαίτερη στήλη θα πρέπει να αναγράφεται ο αναλογούν ΦΠΑ. Σε περίπτωση που αναφέρεται εσφαλμένος ΦΠΑ, αυτός θα διορθώνεται από το Νοσοκομείο.*<br>➢ *Για τη σύγκριση των Προσφορών θα λαμβάνεται υπόψη η τιμή **χωρίς** ΦΠΑ.*<br><br>**** Ε Π Ι Σ Η Μ Α Ν Σ Ε ΙΣ:***<br>***Α)*** **Η προσφορά πρέπει να συνοδεύετε από Υπεύθυνη δήλωση** (όπως εκάστοτε ισχύει σε εφαρμογή και των άρθρων 1 & 3 του Ν. 4250/26-03-2014 (ΦΕΚ74/Α/26.03.2014) του Ν. 1599/1986), στην οποία αναλυτικά θα πρέπει να αναγράφονται τα πλήρη στοιχεία του υποψηφίου καθώς και τα στοιχεία του διαγωνισμού, στον οποίο συμμετέχουν οι οικονομικοί φορείς , και στην οποία θα πρέπει να δηλώνεται ότι:<br><br>• Μέχρι και την ημέρα υποβολής της προσφοράς δεν συντρέχει για τους προσφέροντες λόγος αποκλεισμού από τους αναφερόμενους στα άρθρα 73 (ειδικά παρ. 1, 2 και 4) και 74 του Ν 4412/2016 όπως τροποποιήθηκε και ισχύει, για τους οποίους οι οικονομικοί φορείς αποκλείονται από την συμμετοχή τους σε διαγωνισμούς του Δημοσίου.<br>• Τηρούν όλους τους Ελληνικούς Νόμους, τους σχετικούς με την εργασία (Εργατική – Ασφαλιστική Νομοθεσία).<br>• Έλαβαν γνώση των όρων της πρόσκλησης και τους αποδέχονται πλήρως και ανεπιφύλακτα.<br>• Η Προσφορά συντάχθηκε σύμφωνα με της όρους της παρούσας |

| | |
|---|---|
| | Πρόσκλησης των οποίων οι προσφέροντες έλαβαν πλήρη και ανεπιφύλακτη γνώση.<br>• Δεν έχουν καταδικαστεί για αδίκημα που αφορά την επαγγελματική τους διαγωγή βάσει απόφασης που έχει ισχύ δεδικασμένου, και ότι δεν έχουν διαπράξει βαρύ επαγγελματικό παράπτωμα.<br>• Δεν έχουν καταδικασθεί με αμετάκλητη απόφαση για κάποιο αδίκημα από τα αδικήματα του Αγορανομικού Κώδικα σχετικά με την άσκηση της επαγγελματικής τους δραστηριότητας εφόσον ορίζεται στην πρόσκληση ή κάποιο από τα αδικήματα της υπεξαίρεσης, της απάτης, της εκβίασης, της πλαστογραφίας, της ψευδορκίας και της δόλιας χρεοκοπίας.<br>• Είναι εγγεγραμμένοι στο οικείο επιμελητήριο.<br>• Τα στοιχεία που αναφέρονται στην προσφορά είναι αληθή και ακριβή.<br>• Παραιτούνται από κάθε δικαίωμα αποζημίωσής τους σχετικά με οποιαδήποτε απόφαση της Υπηρεσίας για αναβολή, ματαίωση ή ακύρωση του Διαγωνισμού.<br>• Δεν θα ενεργήσουν αθέμιτα, παράνομα ή καταχρηστικά καθ' όλη τη διάρκεια της διαδικασίας ανάθεσης αλλά και κατά το στάδιο εκτέλεσης της σύμβασης εφόσον επιλεγούν.<br>• Λαμβάνουν τα κατάλληλα μέτρα για να διαφυλάξουν την εμπιστευτικότητα των πληροφοριών που έχουν χαρακτηριστεί ως τέτοιες.<br>• Κατά τη διάρκεια εκτέλεσης της σύμβασης δεσμεύονται για την απαρέγκλιτη τήρηση των διατάξεων του με αρ. 2016/679 Κανονισμού (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 21ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.<br>• Αναλαμβάνουν την υποχρέωση να προσκομίσουν κάθε σχετικό δικαιολογητικό, εφόσον τους ζητηθεί.<br>**Β)** Οι οικονομικοί φορείς δύνανται στην προσφορά τους να συμπεριλάβουν και χωριστό φάκελο με τα δικαιολογητικά κατακύρωσης όπως αυτά περιγράφονται παρακάτω. |
| **ΑΠΟΣΦΡΑΓΙΣΗ ΠΡΟΣΦΟΡΩΝ:** | *Η αποσφράγιση των προσφορών θα γίνει την 4η Μαϊου 2022 ημέρα Τετάρτη και ώρα 10.00 π.μ, στο Γραφείο Προμηθειών του Νοσοκομείου, ενώπιον αρμόδιας Επιτροπής παρουσία των προσφερόντων ή των νομίμως εξουσιοδοτημένων εκπροσώπων τους εφόσον το επιθυμούν.*<br>*Οι οικονομικοί φορείς μπορούν να λάβουν γνώση των λοιπών προσφορών την ημέρα αποσφράγισής τους έως και την επομένη.* |
| **ΑΞΙΟΛΟΓΗΣΗ ΠΡΟΣΦΟΡΩΝ– ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΚΑΤΑΚΥΡΩΣΗΣ** | Η Επιτροπή διενέργειας και αξιολόγησης, προβαίνει στην αξιολόγηση των προσφορών και συντάσσει πρακτικό αξιολόγησης με το οποίο προτείνει την κατακύρωση σε συγκεκριμένο ανάδοχο.<br>Μετά την αξιολόγηση των προσφορών, ο προσφέρων στον οποίο πρόκειται να γίνει η κατακύρωση, εντός αποκλειστικής προθεσμίας δέκα (10) ημερών από την κοινοποίηση της σχετικής έγγραφης ειδοποίησης οφείλει να υποβάλει σε σφραγισμένο φάκελο τα δικαιολογητικά κατακύρωσης που περιγράφονται παρακάτω, στον οποίο να αναγράφονται ευκρινώς τα κάτωθι:<br>• **«ΦΑΚΕΛΟΣ ΔΙΚΑΙΟΛΟΓΗΤΙΚΩΝ ΠΟΥ ΥΠΟΒΑΛΛΟΝΤΑΙ ΚΑΤΑ ΤΟ ΣΤΑΔΙΟ ΤΗΣ ΚΑΤΑΚΥΡΩΣΗΣ ΤΗΣ ΥΠ΄ 71/2022 ΠΡΟΣΚΛΗΣΗΣ ΓΙΑ ΤΗΝ** |

**ΑΝΑΘΕΣΗ ΤΩΝ ΥΠΗΡΕΣΙΩΝ DPO ΣΤΟ ΠΛΑΙΣΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (CPV: 72322000-8) ΓΙΑ ΧΡΟΝΙΚΟ ΔΙΑΣΤΗΜΑ ΕΝΟΣ (1) ΕΤΟΥΣ ΜΕ ΔΙΚΑΙΩΜΑ ΠΡΟΑΙΡΕΣΗΣ ΓΙΑ ΕΝΑ (1) ΕΠΙΠΛΕΟΝ ΕΤΟΣ, ΣΥΝΟΛΙΚΗΣ ΠΡΟΫΠΟΛΟΓΙΖΟΜΕΝΗΣ ΔΑΠΑΝΗΣ 30.000,00€ ΧΩΡΙΣ ΦΠΑ (15.000 € ΧΩΡΙΣ ΦΠΑ ΚΑΙ 18.600,00 € ΜΕ Φ.Π.Α. 24% ΓΙΑ ΕΝΑ (1) ΕΤΟΣ), Η ΟΠΟΙΑ ΜΕ ΦΠΑ 24% ΔΙΑΜΟΡΦΩΝΕΤΑΙ ΣΕ 37.200,00€.**

- Τα στοιχεία του Οικονομικού Φορέα
- Η διευκρίνιση να μην ανοιχθεί από την ταχυδρομική υπηρεσία ή τη γραμματεία

Ο φάκελος να κατατεθεί στο Γραφείο Προμηθειών του Νοσοκομείου, επί της οδού Κωνσταντινουπόλεως 49, ΤΚ 546 42 Θεσσαλονίκη. Με την παράδοση του φακέλου ο παραδίδων τον φάκελο θα παραλαμβάνει από το Γραφείο Προμηθειών απόδειξη παραλαβής του φακέλου στην οποία θα αναγράφονται τα στοιχεία του Οικονομικού Φορέα, η ημερομηνία και η ώρα παραλαβής του φακέλου και θα υπογράφεται από τον αρμόδιο υπάλληλο του Νοσοκομείου που παραλαμβάνει τον φάκελο και τον παραδίδων αυτόν. Το Νοσοκομείο δεν αναλαμβάνει καμία ευθύνη για τυχόν καθυστέρηση στην άφιξη του φακέλου, από οποιαδήποτε αιτία. Ο φάκελος που είτε υποβλήθηκε μετά την καθορισμένη ημερομηνία είτε δεν έφθασε έγκαιρα στο Νοσοκομείο, θα επιστρέφεται στον Προσφέροντα χωρίς να έχει αποσφραγισθεί.

Α) Όσον αφορά την παράγραφο 1 του άρθρου 73, Απόσπασμα του σχετικού μητρώου, όπως του ποινικού μητρώου ή, ελλείψει αυτού, ισοδύναμου εγγράφου που εκδίδεται από αρμόδια δικαστική ή διοικητική αρχή του κράτους – μέλους ή της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο εν λόγω οικονομικός φορέας, από το οποίο προκύπτει ότι πληρούνται αυτές οι προϋποθέσεις. Η υποχρέωση προσκόμισης του ως άνω αποσπάσματος αφορά και τα πρόσωπα του δεύτερου εδαφίου της παραγράφου 1 του άρθρου 73,

Β) Όσον αφορά την παράγραφο 2 του άρθρου 73, πιστοποιητικό που εκδίδεται από την αρμόδια αρχή του οικείου κράτους – μέλους ή χώρας, από το οποίο να προκύπτει ότι είναι ενήμεροι ως προς τις υποχρεώσεις τους που αφορούν τις εισφορές κοινωνικής ασφάλισης (κύριας και επικουρικής) και ως προς τις φορολογικές τους υποχρεώσεις.

Γ) αφορά την παράγραφο 4, περίπτωση β΄ του άρθρου 73, πιστοποιητικό που εκδίδεται από την αρμόδια αρχή του οικείου κράτους - μέλους ή χώρας, από το οποίο προκύπτει ότι δεν τελεί υπό πτώχευση ή έχει υπαχθεί σε διαδικασία εξυγίανσης ή ειδικής εκκαθάρισης, ή τελεί υπό αναγκαστική διαχείριση από εκκαθαριστή ή από το δικαστήριο ή έχει υπαχθεί σε διαδικασία πτωχευτικού συμβιβασμού, ή έχει αναστείλει τις

| | |
|---|---|
| | επιχειρηματικές του δραστηριότητες ή εάν βρίσκεται σε οποιαδήποτε ανάλογη κατάσταση προκύπτουσα από παρόμοια διαδικασία, προβλεπόμενη σε εθνικές διατάξεις νόμου.<br>Αν το κράτος – μέλος ή η χώρα του οικονομικού φορέα δεν εκδίδει τα έγγραφα ή πιστοποιητικά ή όπου τα έγγραφα ή τα πιστοποιητικά δεν καλύπτουν όλες τις ως άνω περιπτώσεις Α) – Γ) (όπως αυτά αναφέρονται και στις παραγράφους 1 και 2 και στην περίπτωση β΄ της παραγράφου 4 του άρθρου 73 του Ν. 4412/2016), τα έγγραφα ή τα πιστοποιητικά μπορεί να αντικαθίσταται από ένορκη βεβαίωση ή, στα κράτη – μέλη ή στις χώρες όπου δεν προβλέπεται ένορκη βεβαίωση, από υπεύθυνη δήλωση του ενδιαφερόμενου ενώπιον αρμόδιας δικαστικής ή διοικητικής αρχής, συμβολαιογράφου ή αρμόδιου επαγγελματικού ή εμπορικού οργανισμού του κράτους – μέλους ή της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο οικονομικός φορέας.<br>Δ) Για την απόδειξη της απαίτησης της παραγράφου 1$^{α}$) και 2 του άρθρου 75, Πιστοποιητικό / βεβαίωση του οικείου επαγγελματικού μητρώου του Παραρτήματος XI του Προσαρτήματος Α΄ του Ν. 4412/2016, με το οποίο πιστοποιείται η εγγραφή του οικονομικού φορέα σε αυτό.<br>**Στην περίπτωση Ένωσης Οικονομικών φορέων, όπου υποβάλλουν κοινή προσφορά, τα παραπάνω κατά περίπτωση δικαιολογητικά υποβάλλονται για κάθε οικονομικό φορέα που συμμετέχει στην Ένωση.**<br>Μετά την ολοκλήρωση του ελέγχου των δικαιολογητικών κατακύρωσης η επιτροπή αξιολόγησης συντάσσει το σχετικό πρακτικό το οποίο μαζί με το Πρακτικό αξιολόγησης επικυρώνονται με σχετική Απόφαση του Διοικητή του Νοσοκομείου.<br>Η Απόφαση αυτή μαζί με τα πρακτικά κοινοποιούνται σε όλους τους συμμετέχοντες. Στη συνέχεια, καλείται ο προσωρινός Ανάδοχος για την υπογραφή της Σύμβασης και την κατάθεση εγγυητικής επιστολής καλής εκτέλεσης της σύμβασης, ίση με το 4% της συμβατικής αξίας χωρίς Φ.Π.Α., χρονικής διάρκειας δέκα τριών (13) μηνών. |
| **ΚΡΙΤΗΡΙΟ ΚΑΤΑΚΥΡΩΣΗΣ:** | Η πλέον συμφέρουσα από οικονομική άποψη προσφορά, μόνο βάσει τιμής. |
| **ΔΙΑΡΚΕΙΑ ΙΣΧΥΟΣ ΠΡΟΣΦΟΡΩΝ:** | Οι Προσφορές ισχύουν και δεσμεύουν τους συμμετέχοντες **για εκατόν είκοσι (120) ημέρες** από την επόμενη μέρα της καταληκτικής ημερομηνίας υποβολής τους.<br>Προσφορά που ορίζει μικρότερο χρόνο ισχύος **απορρίπτεται ως απαράδεκτη.** |
| | |

**ΓΝΘ ΙΠΠΟΚΡΑΤΕΙΟ**

**ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ**

**ΥΠ΄ΑΡΙΘΜ. 71/28-04-2022**

**ΓΙΑ ΤΗΝ ΑΝΑΘΕΣΗ ΤΩΝ ΥΠΗΡΕΣΙΩΝ DPO ΣΤΟ ΠΛΑΙΣΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (CPV: 72322000-8) ΓΙΑ ΧΡΟΝΙΚΟ ΔΙΑΣΤΗΜΑ ΕΝΟΣ (1) ΕΤΟΥΣ ΜΕ ΔΙΚΑΙΩΜΑ ΠΡΟΑΙΡΕΣΗΣ ΓΙΑ ΕΝΑ (1) ΕΠΙΠΛΕΟΝ ΕΤΟΣ , ΣΥΝΟΛΙΚΗΣ ΠΡΟΫΠΟΛΟΓΙΖΟΜΕΝΗΣ ΔΑΠΑΝΗΣ 30.000,00€ ΧΩΡΙΣ ΦΠΑ , Η ΟΠΟΙΑ ΜΕ ΦΠΑ 24% ΔΙΑΜΟΡΦΩΝΕΤΑΙ ΣΕ 37.200,00€**

| | |
|---|---|
| **ΔΗΜΟΣΙΕΥΣΗ:** | Η παρούσα Πρόσκληση αναρτάται:<br>○ Στην ιστοσελίδα του ΓΝΘ ΙΠΠΟΚΡΑΤΕΙΟ(www.ippokratio.gr)<br>○ Στο Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων της Γενικής Γραμματείας Εμπορίου, Κ.Η.Μ.Δ.Η.Σ. |

Θεσσαλονίκη, 28 / 04 / 2022

Ο ΔΙΟΙΚΗΤΗΣ ΤΟΥ ΝΟΣΟΚΟΜΕΙΟΥ

NIKOLAOS ANTONAKIS NIKOLAOS ANTONAKIS Apr 28 2022 4:09 PM

ΝΙΚΟΛΑΟΣ ΑΝΤΩΝΑΚΗΣ

**ΠΑΡΑΡΤΗΜΑ Ι**

**ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ**

**ΕΡΓΟ 1**

## Εφαρμογή του Γενικού Κανονισμού για την Προστασία Δεδομένων (General Data Protection Regulation)

### Άρθρο 1
### Ο νέος Ευρωπαϊκός Κανονισμός Προστασίας Προσωπικών Δεδομένων, 679/2016 (GDPR)

**Γενικά**

Ο Ευρωπαϊκός Κανονισμός Προστασίας Προσωπικών Δεδομένων, 679/2016 (GDPR) -*Κανονισμός*-, ψηφίστηκε στις 27.04.2016, και ισχύει καθολικά, υποχρεωτικά και άμεσα από την 25/05/2018 για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, χωρίς την ανάγκη ψήφισης τοπικής εθνικής νομοθεσίας.

Αντικείμενο του κανονισμού αποτελεί η διαμόρφωση ενός ενιαίου κανονιστικού πλαισίου για την επεξεργασία κάθε είδους προσωπικών δεδομένων, αυτοματοποιημένη ή μη, στα κράτη μέλη της Ευρωπαϊκής Ένωσης και εισάγει μια σειρά διαδικασιών και υποχρεώσεων για την:

- Συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα σε όλο τον κύκλο ζωής τους.
- Την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των δεδομένων προσωπικού χαρακτήρα.
- Τις ενέργειες σε περίπτωση παραβίασης.

Η εφαρμογή του αυξάνει σημαντικά τις απαιτήσεις που τίθενται στους οργανισμούς που επεξεργάζονται προσωπικά δεδομένα, καθώς το μέγεθος των κυρώσεων σε περίπτωση παραβάσεων και αποκλίσεων, είναι πολύ ψηλό.

**Πεδίο Εφαρμογής**

Ο Κανονισμός έχει εφαρμογή σε **όλους τους οργανισμούς** (ιδιωτικές και δημόσιες επιχειρήσεις, κρατικές αρχές, συλλόγους, κλπ.) 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.

**Υποχρεώσεις Φορέα**

Ο κάθε φορέας υποχρεώνεται από τον κανονισμό:

- Να μεριμνήσει για όλα τα τεχνικά και οργανωτικά μέτρα που θα διασφαλίζουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα σύμφωνα με τα οριζόμενα στον Κανονισμό

- Να αναπτύξει πολιτικές προστασίας των δεδομένων προσωπικού χαρακτήρα σύμφωνα με τα οριζόμενα στον Κανονισμό
- Να αποδείξει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται σύμφωνα με τον Κανονισμό

Ιδιαίτερα στην περίπτωση των προσωπικών δεδομένων ειδικής κατηγορίας (ευαίσθητα προσωπικά δεδομένων) προβλέπονται επιπλέον απαιτήσεις, όπως η υποχρέωση για τεκμηρίωση των σχετικών διαδικασιών, ο ορισμός Υπευθύνου Προστασίας Δεδομένων (DPO), η διενέργεια εκτίμησης αντικτύπου, κ.ά.

Για τον λόγο αυτό το ΓΝΘ «Ιπποκράτειο» -*Νοσοκομείο*- προχωρά στην ανάδειξη αναδόχου παροχής υπηρεσιών οργάνωσης, εφαρμογής και παρακολούθησης του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation).

**Άρθρο 2**

**Τεχνικές Προδιαγραφές**

**Αντικείμενο του Έργου**

Αντικείμενο του αναδόχου είναι:

1. Ο έλεγχος του επιπέδου εφαρμογής του Γενικού Κανονισμού έως σήμερα.
2. Η επικαιροποίηση των σχετικών αναγκών του Νοσοκομείου και των ανάλογων πολιτικών του.
3. Η επικαιροποίηση και υλοποίηση σχεδίου δράσεως/ενεργειών/διαδικασιών, μαζί με την απαραίτητη τεκμηρίωση, προκειμένου να επιτευχθεί η συνεχής συμμόρφωση του Νοσοκομείου με τον Κανονισμό.
4. Η παροχή υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (DPO)

Οι προτεινόμενες ελάχιστες φάσεις υλοποίησης του έργου είναι οι ακόλουθες:

Φάση 1: Προετοιμασία του έργου – Έλεγχος επιπέδου εναρμόνισης με τον Κανονισμό- Εγκατάσταση Υπευθύνου Προστασίας Δεδομένων (DPO)

Φάση 2: Ορισμός πλαισίου εργασίας – Επικαιροποίηση πολιτικών GDPR – Ενημέρωση φορέα

Φάση 3: Επικαιροποίηση και κατάθεση σχεδίου δράσης συνεχούς συμμόρφωσης - Ενημέρωση

Φάση 4: Υλοποίηση του Σχεδίου Δράσης – Συνεχής εκπαίδευση

Φάση 5: Επιθεώρηση Συμμόρφωσης – Συνεχής παρουσίαση αποτελεσμάτων

Υπηρεσίες DPO: Εγκατάσταση υπεύθυνου DPO

Ο ανάδοχος μπορεί να ακολουθήσει οποιαδήποτε οργάνωση για την πρόταση του αρκεί να περιλαμβάνει κατ’ ελάχιστον τις υπηρεσίες που αναφέρονται.

Απαραίτητη προϋπόθεση η συνεχής επικοινωνία του αναδόχου με τον φορέα και η φυσική παρουσία του σε αυτόν τουλάχιστον 5 ημέρες /μήνα.

**Φάση 1 - Προετοιμασία του έργου – Έλεγχος επιπέδου εναρμόνισης με τον Κανονισμό**

**1.1 Ενέργειες**

Το έργο της εναρμόνισης του Νοσοκομείου με τις απαιτήσεις του Κανονισμού είναι πολυσύνθετο καθώς η πλήρης και συνεχόμενη εναρμόνιση με τον Κανονισμό δεν επιτυγχάνεται μόνο με οργανωτικά ή τεχνολογικά μέτρα αλλά πρωτίστως με την δημιουργία της κατάλληλης κουλτούρας για την προστασία των δεδομένων προσωπικού χαρακτήρα μέσα στον οργανισμό. Απαραίτητη επίσης είναι η ρητή δέσμευση της Διοίκησης προς την κατεύθυνσης της προστασίας των δεδομένων προσωπικού χαρακτήρα και της εναρμόνισης με τον κανονισμό.

Το Νοσοκομείο έχει ήδη εφαρμόσει πρόγραμμα ευαισθητοποίησης και εκπαίδευσης του προσωπικού και των Υπηρεσιών του, διάρκειας 18 μηνών. Κατά το διάστημα του σταδίου αυτού ο ανάδοχος θα πρέπει να ελέγξει το επίπεδο προετοιμασίας αλλά και εφαρμογής του Κανονισμού στο σύνολο του Νοσοκομείου. Σε συνεργασία με τη Διοίκηση του Νοσοκομείου θα πρέπει επιτύχουν κοινή καταγραφή και αντίληψη των απαιτήσεων του έργου, της μεθοδολογίας και του χρονοδιαγράμματος υλοποίησης του έργου. Το Νοσοκομείο θα ορίσει τη δική του ομάδα έργου σύμφωνα με τα οριζόμενα στο προοίμιο του παρόντος.

Συγκεκριμένα, σε αυτή την φάση θα πρέπει να γίνουν τουλάχιστον οι παρακάτω ενέργειες:

- Έλεγχος της υφιστάμενης κατάστασης σε όλα τα Τμήματα και Κλινικές του Νοσοκομείου
- Αναφορά προς τη Διοίκηση για το επίπεδο εφαρμογής των Πολιτικών
- Παρουσίαση στην Διοίκηση των αναγκών για τη συνέχεια.
- Οριστικοποίηση του σχεδίου υλοποίησης του έργου καθώς και των χρονοδιαγραμμάτων με βάση τις απαιτήσεις του Νοσοκομείου.

**1.2. Εγκατάσταση Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO)**

Από την εκκίνηση της φάσης αυτής ο ανάδοχος θα τοποθετήσει – ενεργοποιήσει τον Υπεύθυνο Προστασίας Προσωπικών δεδομένων (DPO). Οι υποχρεώσεις-ευθύνες του DPO και της ομάδας εργασίας του αναφέρονται αναλυτικά στον Γενικό Κανονισμό.

**1.3. Παραδοτέα**

- Έκθεση επιπέδου εφαρμογής των πολιτικών και εναρμόνισης του Νοσοκομείου με τον Κανονισμό
- Παρουσίαση του Κανονισμού και των απαιτήσεων για την εφαρμογή του.

**<u>Φάση 2- Ορισμός πλαισίου εργασίας – Επικαιροποίηση πολιτικών GDPR – Εγκατάσταση Υπευθύνου Προστασίας Δεδομένων (DPO) – Ενημέρωση φορέα</u>**

**2.1. Ενέργειες**

1. Θα πρέπει από τον ανάδοχο να γίνει έλεγχος και επικαιροποίηση των πολιτικών που έχουν εγκριθεί από το Νοσοκομείο.

2. Θα πρέπει να επικαιροποιηθεί ο κύκλος ζωής των δεδομένων προσωπικού χαρακτήρα, και ιδιαίτερα των προσωπικών δεδομένων ειδικής κατηγορίας, σε όλα τα

τμήματα του Νοσοκομείου. Η επικαιροποίηση θα αφορά και τα απαραίτητα αρχεία τεκμηρίωσης που πρέπει να έχει στην κατοχή του το Νοσοκομείο σε σχέση τον Κανονισμό. Σαν τέτοια, ενδεικτικά αναφέρονται:

* Κατάλογος δεδομένων προσωπικού χαρακτήρα που συλλέγονται και χρησιμοποιούνται, ο τρόπος χρήσης και αποθήκευσης τους, η ροή τους, η προστασία τους και τα δικαιώματα πρόσβασης, η διαδικασία λήψης συγκατάθεσης κλπ. Η καταγραφή των δεδομένων θα πρέπει να είναι λεπτομερής και θα αφορά τόσο τα έντυπα όσο και τα ηλεκτρονικά μέσα στα οποία μπορούν βρεθούν προσωπικά δεδομένων, όπως έγγραφα, φόρμες, κατάλογοι αρχεία κλπ.
* Ταξινόμηση των δεδομένων προσωπικού χαρακτήρα ανά τύπο (π.χ. ειδικής κατηγορίας, δημόσια κλπ)
* Διαγράμματα ροής για την διακίνηση των δεδομένων προσωπικού χαρακτήρα μέσα στο Νοσοκομείο καθώς και εκτός Νοσοκομείου (συμβόλαια συντήρησης κλπ)
* Αιτιολόγηση αναγκαιότητας λήψης και διατήρησης τους, διότι λόγω της ιδιαιτερότητας του Νοσοκομείου για την εκπλήρωση του σκοπού του απαιτείται η συλλογή και επεξεργασία πλήθους δεδομένων προσωπικού χαρακτήρα.

**Απογραφή των δεδομένων προσωπικού χαρακτήρα / κατηγοριοποίηση**

Επικαιροποίηση θα πρέπει να γίνει στο σύνολο των δραστηριοτήτων επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του Νοσοκομείου. Οι ενέργειες αυτές πρέπει να καλύπτουν τουλάχιστον τις απαιτήσεις του άρθρου 30, και αποτυπώνουν κατ' ελάχιστον:

- Το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου υπαλλήλου επεξεργασίας και του υπεύθυνου προστασίας των δεδομένων
- Την θέση των δεδομένων
- Τον όγκο και την μορφή των πληροφοριών (πλήθος εγγραφών, πλήθος εγγράφων, αριθμού σελίδων κλπ, χαρτί ή ηλεκτρονικό; δομημένο ή αδόμητο)
- Τους σκοπούς της επεξεργασίας και τις ανάγκες που καλύπτουν
- Την κατηγορία των δεδομένων
- Την περιγραφή των δεδομένων (π.χ. όνομα, φυσική διεύθυνση, διεύθυνση ηλεκτρονικού ταχυδρομείου, αναγνωριστικό ταυτότητας (ΑΔΤ, ΑΦΜ, ΑΜΚΑ κλπ), ιατρικό ιστορικό, αποτελέσματα και γνωματεύσεις εξετάσεων κλπ)
- Την κατηγοριοποίηση των προσωπικών στοιχείων ταυτότητας (μη ταυτοποίηση, μερική ταυτοποίηση, ταυτοποίηση, ευαίσθητα προσωπικά δεδομένα κλπ)
- Τις κατηγορίες αποδεκτών στους οποίους έχουν διαβιβαστεί ή πρόκειται να γνωστοποιηθούν τα προσωπικά δεδομένα
- Τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων
- Γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας που αναφέρονται στο άρθρο 32 παράγραφος 1
- Υλικό τεκμηρίωσης που βασίζεται η επεξεργασία
- Όποια άλλα στοιχεία σχετίζονται με την επεξεργασία δεδομένων

**Ανάλυση της συμμόρφωσης**

Μετά την επικαιροποίηση των πιο πάνω 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 συμμόρφωσης του Νοσοκομείου με τον Κανονισδμό.

**Εκτίμηση αντικτύπου (Data Protection Impact Assessment)**

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 τουλάχιστον με βάση το άρθρο 35 παρ. 7:

- Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει το Νοσοκομείο
- Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς
- Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (υποκειμένων των δεδομένων)
- 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.

**Αποτίμηση Επικινδυνότητας (Risk Assessment / Treatment)**

Ο ανάδοχος βασισμένος στην ανάλυση της 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 εξουσιοδοτημένη τροποποίηση ή καταστροφής.

### 2.2. Ενημέρωση φορέα

### 2.3. Παραδοτέα

- Αρχεία Τεκμηρίωσης
- Αρχεία Δραστηριοτήτων Επεξεργασίας
- Ανάλυση συμμόρφωσης ανά άρθρο του Κανονισμού.
- Εκτίμηση αντικτύπου (Data Protection Impact Assessment)
- Αποτίμηση Επικινδυνότητας (Risk Assessment)
- Επικαιροποιημένα κείμενα πολιτικών GDRP

## Φάση 3 - Επικαιροποίηση και κατάθεση σχεδίου δράσης συνεχούς συμμόρφωσης-Ενημέρωση

### 3.1. Ενέργειες

**Εκπόνηση Σχεδίου Δράσης**

Βάση της εκτίμησης επιπέδου συμμόρφωσης, την εκτίμηση αντικτύπου και την αποτίμηση επικινδυνότητας, ο ανάδοχος θα εκπονήσει και θα τεκμηριώσει σχέδιο δράσης για επικαιροποίηση της συμμόρφωσης 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 («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/επικαιροποίηση.

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 τέτοιες 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 Προστασίας 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 συντήρηση και υποστήριξης
- Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές πρόσληψης
- 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 υγείας 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 κλπ) οι οποίες θα προστεθούν στα υπάρχοντα ή νέα συμβόλαια. Ενδεικτικά θα παραλαμβάνει

- 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)

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 της Φάσης 1.

**Παρουσίαση του Σχεδίου Δράσης**

Με την ολοκλήρωση του σχεδίου δράσης, ο ανάδοχος θα το παρουσιάσει μαζί με τα συμπεράσματα της ανάλυσής του, στην Διοίκηση και στα αρμόδια στελέχη του Νοσοκομείου Ο στόχος της παρουσίασης είναι να ενημερωθούν και να ευαισθητοποιηθούν όλα τα εμπλεκόμενα μέρη για το σχέδιο δράσης και τις απαιτήσεις του Κανονισμού και κυρίως για τις αλλαγές στις Πολιτικές / Διαδικασίες που αυτός επιφέρει. Με τον τρόπο αυτό θα διευκολυνθεί η λήψη των απαραίτητων διοικητικών αποφάσεων για την υλοποίηση των απαιτούμενων μέτρων/ενεργειών

Ο Ανάδοχος θα πρέπει στην τελική διαμόρφωση/επικαιροποίηση του σχεδίου δράσης, και πριν την έγκριση του από την Διοίκηση, να λάβει υπόψη τις παρατηρήσεις και προτάσεις των στελεχών. Επίσης θα παρέχει τις ανάλογες υπηρεσίες υποστήριξης με την τεκμηρίωση της αναγκαιότητας των δράσεων.

### 3.2. Παραδοτέα

- Επικαιροποιημένο Σχέδιο Δράσης Συμμόρφωσης με τις απαραίτητες πολιτικές και διαδικασίες, ανά άρθρο του Κανονισμού.

- Σχέδιο συνεχούς συμμόρφωσης-επικαιροποίησης με τον Κανονισμό
- Παρουσίαση του σχεδίου δράσης

**Φάση 4 - Υλοποίηση του Σχεδίου Δράσης – Συνεχής Εκπαίδευση**

**4.1 Ενέργειες**

**Υλοποίηση του σχεδίου δράσης**

Ο ανάδοχος, μετά την έγκριση από την Διοίκηση, έχει υποχρέωση να υλοποιήσει στο 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/επικαιροποίηση 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 εμπλέκονται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

  Ο ανάδοχος είναι υπεύθυνος για την υλοποίηση του σχεδίου δράσης.

**Συνεχής Εκπαίδευση**

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

- Να είναι ενήμερο για τον Κανονισμό, τις απαιτήσεις του και την υποχρέωση του Νοσοκομείου να συμμορφώνεται με αυτόν.
- Να είναι γνώστες 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 γνωρίζουν 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.

**1.4. Παραδοτέα**

- Τεκμηρίωση της υλοποίησης από τον ανάδοχο του Σχεδίου Δράσης.
- Επικαιροποιημένες διαδικασίες και πολιτικές συμμόρφωσης με τον Κανονισμό.
- Πρόγραμμα συνεχούς εκπαίδευσης και ενημέρωσης προσωπικού καθώς και σχετικό εκπαιδευτικό και ενημερωτικό υλικό

## Φάση 5 – Επιθεώρηση Συμμόρφωσης – Παρουσίαση Αποτελεσμάτων

### 5.1. Ενέργειες

Η διαδικασία συμμόρφωσης του Νοσοκομείου με τον Κανονισμό θα πρέπει να αποτελεί διαρκή και ανοιχτή δραστηριότητα τόσο του αναδόχου όσο και του Νοσοκομείου. Κατά τη φάση της επιθεώρησης συμμόρφωσης από τον ανάδοχο θα επιθεωρούνται 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 υπογραφεί, ώστε να επιβεβαιώνεται η διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα και των απαιτήσεων του Κανονισμού.

Επιπλέον, θα επιθεωρούνται 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/Υποστήρικης που έχουν υπογραφεί με τους συνεργάτες, καθώς και το είδος της εκπαίδευσης / ενημέρωσης που έχουν λάβει, όσον αφορά την προστασία των προσωπικών δεδομένων.

Ορόσημα της διαδικασίας τοποθετούνται στο τέλος κάθε φάσης του έργου. Με την συμπλήρωση κάθε ορόσημου ο ανάδοχος θα πρέπει να επικαιροποιεί εάν απαιτείται κα τα παραδοτέα προηγούμενων φάσεων.

Ο ανάδοχος αναλαμβάνει να εκτελέσει όποιο συμπληρωματικό μέτρο / ενέργεια προκύψει και στη συνέχεια να συντάξει τελική έκθεση με τα αποτελέσματα του εσωτερικού ελέγχου.

Τα αποτελέσματα κάθε επιθεώρησης καταγράφονται και φυλάσσονται στο αρχείο του έργου τόσο από τον ανάδοχο όσο και από το Νοσοκομείο, αποτελούν δε περιουσιακό στοιχείο και του Νοσοκομείου.

**Παρουσίαση Αποτελεσμάτων Επιθεώρησης Συμμόρφωσης**

Ο ανάδοχος έχει υποχρέωση παρουσίασης προς τη Διοίκηση του Νοσοκομείου, των αποτελεσμάτων της επιθεώρησης συμμόρφωσης καθώς και του επικαιροποιημένου Data Protection Impact Assessment και Risk Assessment, με γραπτή έκθεση. Η Διοίκηση του Νοσοκομείου διατηρεί τη δυνατότητα να ζητήσει αυτοπρόσωπη παρουσίαση από τον ανάδοχο.

**Τελική Επιθεώρηση υλοποίησης του έργου**

Ο ανάδοχος υποχρεούται σε παρουσίαση προς τη Διοίκηση του Νοσοκομείου, της τελικής εικόνας πορείας του έργου, τρείς (3) μήνες πριν τη λήξη της σύμβασης.

### 5.2. Παραδοτέα

- Επικαιροποιημένο Αρχείο Τεκμηρίωσης
- Επικαιροποιημένα Αρχεία Δραστηριοτήτων Επεξεργασίας

- Επικαιροποιημένη Ανάλυση του επιπέδου συμμόρφωσης του Νοσοκομείου, ανά άρθρο του Κανονισμού.
- Επικαιροποιημένη Εκτίμηση αντικτύπου (Data Protection Impact Assessment)
- Επικαιροποιημένη Αποτίμηση Επικινδυνότητας (Risk Assessment)
- Επικαιροποιημένο Σχέδιο Δράσης Συμμόρφωσης με τα συμπληρωματικά μέτρα και διαδικασίες, ανά άρθρο του Κανονισμού
- Εκθέσεις επιθεωρήσεων
- Τελική παρουσίαση αποτελεσμάτων του έργου

**ΥΠΗΡΕΣΙΕΣ DPO**

Ο ανάδοχος θα παρέχει στον Νοσοκομείο καθόλη τη διάρκεια της σύμβασης κατάλληλα καταρτισμένο και πιστοποιημένο άτομο προκειμένου να αναλάβει τα καθήκοντα του Data Protection Officer (DPO). Ο DPO θα πλαισιώνεται από κατάλληλη υποστηρικτική ομάδα, η οποία θα περιλαμβάνει κατ' ελάχιστο έναν Information Security Consultant, έναν IT Auditor και έναν Νομικό με εμπειρία πάνω σε θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων.

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 αντικτύπου (DPIA) και θα δημιουργεί καινούργιες για επεξεργασίες υψηλού ρίσκου. Ακόμα θα αναλαμβάνει την ενημέρωση του προσωπικού καθώς και τις εσωτερικές επιθεωρήσεις, με σκοπό την επίτευξη του βέλτιστου επιπέδου συμμόρφωσης.

Η δραστηριότητα του DPO θα πρέπει να βρίσκεται σε συνεχή συντονισμό με την Ομάδα Έργου του Νοσοκομείου και το ΑΤΕΠΕΣΕ ως υπεύθυνης υπηρεσίας συντονισμού αυτής.

**Άρθρο 3**

**Χρονοδιάγραμμα Υλοποίησης**

Το χρονοδιάγραμμα Υλοποίησης του έργου Συμμόρφωσης είναι 12 μήνες με προτεινόμενο χρόνο υλοποίησης ανά φάση:

| ΜΗΝΕΣ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Φάση 1 | X | X | X | | | | | | | | | |
| Φάση 2 | | X | X | X | | | | | | | | |
| Φάση 3 | | | X | X | X | | | | | | | |
| Φάση 4 | | | | | X | X | X | X | | | | |
| Φάση 5 | | | | | | | X | X | X | X | X | X |
| Υπηρεσίες DPO | X | X | X | X | X | X | X | X | X | X | X | X |

**Προϋπολογισμός**

15.000€ πλέον ΦΠΑ.

**Άρθρο 4**

**Τεχνική και Επαγγελματική Ικανότητα αναδόχου**

Ο ανάδοχος απαιτείται να

- Έχει υλοποιήσει ή υλοποιεί τουλάχιστον πέντε (5) έργα GDPR
- Να διαθέτει πιστοποίηση κατά ISO 9001 και ISO 27001
- Η προτεινόμενη δική του ομάδα έργου θα πρέπει να περιλαμβάνει κατ' ελάχιστο τις ακόλουθες ειδικότητες
  - Project Manager
  - Information Security Consultant
  - IT Auditor
  - Νομικό Σύμβουλο
- Τα μέλη της ομάδας θα πρέπει να έχουν τουλάχιστον τουλάχιστον 5ετή εμπειρία σε θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων ενώ θα πρέπει να έχουν συμμετάσχει σε δύο (2) τουλάχιστον έργα με αντικείμενο θέματα ασφάλειας πληροφοριών/προσωπικών δεδομένων.
- Ο Information Security Consultant, θα πρέπει να είναι πιστοποιημένος ISO 27001 auditors.

Ένα μέλος της ομάδας θα πρέπει να διαθέτει βεβαίωση ως Data Protection Officer (DPO) από εταιρία πιστοποιήσεων ή αντίστοιχη βεβαίωση άλλου φορέα καθώς και εμπειρία με εμπειρία σε ανάλογη θέση φορέα Β΄ βάθμιας φροντίδας υγείας.

## ΠΑΡΑΡΤΗΜΑ ΙΙ

## ΥΠΟΔΕΙΓΜΑ ΦΥΛΛΟΥ ΣΥΜΜΟΡΦΩΣΗΣ

(Αναλυτικό φύλλο συμμόρφωσης- τεκμηρίωσης, με το οποίο δίνονται αναλυτικές απαντήσεις με σχετικές παραπομπές σε όλα τα σημεία των «Απαιτήσεων- Τεχνικών Προδιαγραφών», καθώς και σε κάθε άλλη τεχνική απαίτηση της Αναθέτουσας Αρχής)

### Υπηρεσίες DPO

| ΠΕΡΙΓΡΑΦΗ ΤΕΧΝΙΚΗΣ ΠΡΟΔΙΑΓΡΑΦΗΣ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ ΥΠΟΨΗΦΙΟΥ | ΠΑΡΑΠΟΜΠΗ ΣΕ ΤΕΧΝΙΚΑ ΦΥΛΛΑΔΙΑ |
|---|---|---|---|
| **Αντικείμενο του Έργου** | | | |
| Αντικείμενο του αναδόχου είναι: | ΝΑΙ | | |
| 5. Ο έλεγχος του επιπέδου εφαρμογής του Γενικού Κανονισμού έως σήμερα. | ΝΑΙ | | |
| 6. Η επικαιροποίηση των σχετικών αναγκών του Νοσοκομείου και των ανάλογων πολιτικών του. | ΝΑΙ | | |
| 7. Η επικαιροποίηση και υλοποίηση σχεδίου δράσεως/ενεργειών/διαδικασιών, μαζί με την απαραίτητη τεκμηρίωση, προκειμένου να επιτευχθεί η συνεχής συμμόρφωση του Νοσοκομείου με τον Κανονισμό. | ΝΑΙ | | |
| 8. Η παροχή υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (DPO) | ΝΑΙ | | |
| Οι προτεινόμενες ελάχιστες φάσεις υλοποίησης του έργου είναι οι ακόλουθες: | ΝΑΙ | | |
| Φάση 1: Προετοιμασία του έργου – Έλεγχος επιπέδου εναρμόνισης με τον Κανονισμό- Εγκατάσταση Υπευθύνου Προστασίας Δεδομένων (DPO) | ΝΑΙ | | |
| Φάση 2: Ορισμός πλαισίου εργασίας – Επικαιροποίηση πολιτικών GDPR – Ενημέρωση φορέα | ΝΑΙ | | |
| Φάση 3: Επικαιροποίηση και κατάθεση σχεδίου δράσης συνεχούς συμμόρφωσης - Ενημέρωση | ΝΑΙ | | |
| Φάση 4: Υλοποίηση του Σχεδίου Δράσης – Συνεχής εκπαίδευση | ΝΑΙ | | |
| Φάση 5: Επιθεώρηση Συμμόρφωσης – Συνεχής | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| παρουσίαση αποτελεσμάτων | | | |
| Υπηρεσίες DPO: Εγκατάσταση υπεύθυνου DPO | ΝΑΙ | | |
| | ΝΑΙ | | |
| Ο ανάδοχος μπορεί να ακολουθήσει οποιαδήποτε οργάνωση για την πρόταση του αρκεί να περιλαμβάνει κατ' ελάχιστον τις υπηρεσίες που αναφέρονται. | ΝΑΙ | | |
| Απαραίτητη προϋπόθεση η συνεχής επικοινωνία του αναδόχου με τον φορέα και η φυσική παρουσία του σε αυτόν τουλάχιστον 5 ημέρες /μήνα. | ΝΑΙ | | |
| | | | |
| **Φάση 1 - Προετοιμασία του έργου – Έλεγχος επιπέδου εναρμόνισης με τον Κανονισμό** | | | |
| | | | |
| **1.2 Ενέργειες** | | | |
| Το έργο της εναρμόνισης του Νοσοκομείου με τις απαιτήσεις του Κανονισμού είναι πολυσύνθετο καθώς η πλήρης και συνεχόμενη εναρμόνιση με τον Κανονισμό δεν επιτυγχάνεται μόνο με οργανωτικά ή τεχνολογικά μέτρα αλλά πρωτίστως με την δημιουργία της κατάλληλης κουλτούρας για την προστασία των δεδομένων προσωπικού χαρακτήρα μέσα στον οργανισμό. Απαραίτητη επίσης είναι η ρητή δέσμευση της Διοίκησης προς την κατεύθυνσης της προστασίας των δεδομένων προσωπικού χαρακτήρα και της εναρμόνισης με τον κανονισμό. | ΝΑΙ | | |
| Το Νοσοκομείο έχει ήδη εφαρμόσει πρόγραμμα ευαισθητοποίησης και εκπαίδευσης του προσωπικού και των Υπηρεσιών του, διάρκειας 18 μηνών. Κατά το διάστημα του σταδίου αυτού ο ανάδοχος θα πρέπει να ελέγξει το επίπεδο προετοιμασίας αλλά και εφαρμογής του Κανονισμού στο σύνολο του Νοσοκομείου. Σε συνεργασία με τη Διοίκηση του Νοσοκομείου θα πρέπει επιτύχουν κοινή καταγραφή και αντίληψη των απαιτήσεων του έργου, της μεθοδολογίας και του χρονοδιαγράμματος υλοποίησης του έργου. Το Νοσοκομείο θα ορίσει τη δική του ομάδα έργου σύμφωνα με τα οριζόμενα στο προοίμιο του παρόντος. | ΝΑΙ | | |
| Συγκεκριμένα, σε αυτή την φάση θα πρέπει να γίνουν τουλάχιστον οι παρακάτω ενέργειες: | ΝΑΙ | | |
| • Έλεγχος της υφιστάμενης κατάστασης σε όλα τα Τμήματα και Κλινικές του Νοσοκομείου | ΝΑΙ | | |
| • Αναφορά προς τη Διοίκηση για το επίπεδο εφαρμογής των Πολιτικών | ΝΑΙ | | |
| • Παρουσίαση στην Διοίκηση των αναγκών για τη | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| συνέχεια. | | | |
| • Οριστικοποίηση του σχεδίου υλοποίησης του έργου καθώς και των χρονοδιαγραμμάτων με βάση τις απαιτήσεις του Νοσοκομείου. | ΝΑΙ | | |
| | | | |
| **1.5. Εγκατάσταση Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO)** | | | |
| Από την εκκίνηση της φάσης αυτής ο ανάδοχος θα τοποθετήσει – ενεργοποιήσει τον Υπεύθυνο Προστασίας Προσωπικών δεδομένων (DPO). Οι υποχρεώσεις-ευθύνες του DPO και της ομάδας εργασίας του αναφέρονται αναλυτικά στον Γενικό Κανονισμό. | ΝΑΙ | | |
| | | | |
| **1.6. Παραδοτέα** | | | |
| • Έκθεση επιπέδου εφαρμογής των πολιτικών και εναρμόνισης του Νοσοκομείου με τον Κανονισμό | ΝΑΙ | | |
| • Παρουσίαση του Κανονισμού και των απαιτήσεων για την εφαρμογή του. | ΝΑΙ | | |
| | | | |
| | | | |
| **Φάση 2- Ορισμός πλαισίου εργασίας – Επικαιροποίηση πολιτικών GDPR – Εγκατάσταση Υπευθύνου Προστασίας Δεδομένων (DPO) – Ενημέρωση φορέα** | | | |
| | | | |
| **2.1. Ενέργειες** | | | |
| 1. Θα πρέπει από τον ανάδοχο να γίνει έλεγχος και επικαιροποίηση των πολιτικών που έχουν εγκριθεί από το Νοσοκομείο. | ΝΑΙ | | |
| 2. Θα πρέπει να επικαιροποιηθεί ο κύκλος ζωής των δεδομένων προσωπικού χαρακτήρα, και ιδιαίτερα των προσωπικών δεδομένων ειδικής κατηγορίας, σε όλα τα τμήματα του Νοσοκομείου. Η επικαιροποίηση θα αφορά και τα απαραίτητα αρχεία τεκμηρίωσης που πρέπει να έχει στην κατοχή του το Νοσοκομείο σε σχέση τον Κανονισμό. Σαν τέτοια, ενδεικτικά αναφέρονται: | ΝΑΙ | | |
| * Κατάλογος δεδομένων προσωπικού χαρακτήρα που συλλέγονται και χρησιμοποιούνται, ο τρόπος χρήσης και αποθήκευσης τους, η ροή τους, η προστασία τους και τα δικαιώματα πρόσβασης, η διαδικασία λήψης συγκατάθεσης κλπ. Η καταγραφή των δεδομένων θα πρέπει να είναι λεπτομερής και θα αφορά τόσο τα έντυπα όσο και τα | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| ηλεκτρονικά μέσα στα οποία μπορούν βρεθούν προσωπικά δεδομένων, όπως έγγραφα, φόρμες, κατάλογοι αρχεία κλπ. | | | |
| * Ταξινόμηση των δεδομένων προσωπικού χαρακτήρα ανά τύπο (π.χ. ειδικής κατηγορίας, δημόσια κλπ) | ΝΑΙ | | |
| * Διαγράμματα ροής για την διακίνηση των δεδομένων προσωπικού χαρακτήρα μέσα στο Νοσοκομείο καθώς και εκτός Νοσοκομείου (συμβόλαια συντήρησης κλπ) | ΝΑΙ | | |
| * Αιτιολόγηση αναγκαιότητας λήψης και διατήρησης τους, διότι λόγω της ιδιαιτερότητας του Νοσοκομείου για την εκπλήρωση του σκοπού του απαιτείται η συλλογή και επεξεργασία πλήθους δεδομένων προσωπικού χαρακτήρα. | ΝΑΙ | | |
| | | | |
| **Απογραφή των δεδομένων προσωπικού χαρακτήρα / κατηγοριοποίηση** | | | |
| Επικαιροποίηση θα πρέπει να γίνει στο σύνολο των δραστηριοτήτων επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του Νοσοκομείου. Οι ενέργειες αυτές πρέπει να καλύπτουν τουλάχιστον τις απαιτήσεις του άρθρου 30, και αποτυπώνουν κατ' ελάχιστον: | ΝΑΙ | | |
| • Το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου υπαλλήλου επεξεργασίας και του υπεύθυνου προστασίας των δεδομένων | ΝΑΙ | | |
| • Την θέση των δεδομένων | ΝΑΙ | | |
| • Τον όγκο και την μορφή των πληροφοριών (πλήθος εγγραφών, πλήθος εγγράφων, αριθμού σελίδων κλπ, χαρτί ή ηλεκτρονικό; δομημένο ή αδόμητο) | ΝΑΙ | | |
| • Τους σκοπούς της επεξεργασίας και τις ανάγκες που καλύπτουν | ΝΑΙ | | |
| • Την κατηγορία των δεδομένων | ΝΑΙ | | |
| • Την περιγραφή των δεδομένων (π.χ. όνομα, φυσική διεύθυνση, διεύθυνση ηλεκτρονικού ταχυδρομείου, αναγνωριστικό ταυτότητας (ΑΔΤ, ΑΦΜ, ΑΜΚΑ κλπ), ιατρικό ιστορικό, αποτελέσματα και γνωματεύσεις εξετάσεων κλπ) | ΝΑΙ | | |
| • Την κατηγοριοποίηση των προσωπικών στοιχείων ταυτότητας (μη ταυτοποίηση, μερική ταυτοποίηση, ταυτοποίηση, ευαίσθητα προσωπικά δεδομένα κλπ) | ΝΑΙ | | |
| • Τις κατηγορίες αποδεκτών στους οποίους έχουν διαβιβαστεί ή πρόκειται να γνωστοποιηθούν τα προσωπικά δεδομένα | ΝΑΙ | | |
| • Τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων | ΝΑΙ | | |
| • Γενική περιγραφή των τεχνικών και οργανωτικών | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| μέτρων ασφαλείας που αναφέρονται στο άρθρο 32 παράγραφος 1 | | | |
| • Υλικό τεκμηρίωσης που βασίζεται η επεξεργασία | ΝΑΙ | | |
| • Όποια άλλα στοιχεία σχετίζονται με την επεξεργασία δεδομένων | ΝΑΙ | | |
| | | | |
| **Ανάλυση της συμμόρφωσης** | | | |
| Μετά την επικαιροποίηση των πιο πάνω 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. | ΝΑΙ | | |
| 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. | ΝΑΙ | | |
| Η αποτίμηση του βαθμού υλοποίησης θα προσδιορίσει τον βαθμό της συμμόρφωσης του Νοσοκομείου με τον Κανονισδμό. | ΝΑΙ | | |
| | | | |
| **Εκτίμηση αντικτύπου (Data Protection Impact Assessment)** | | | |
| 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 τουλάχιστον με βάση το άρθρο 35 παρ. 7: | ΝΑΙ | | |
| • Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει το Νοσοκομείο | ΝΑΙ | | |
| • Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| • Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (υποκειμένων των δεδομένων) | ΝΑΙ | | |
| • 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. | ΝΑΙ | | |
| | | | |
| **Αποτίμηση Επικινδυνότητας (Risk Assessment / Treatment)** | | | |
| Ο ανάδοχος βασισμένος στην ανάλυση της 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. | ΝΑΙ | | |
| 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. | ΝΑΙ | | |
| 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. | ΝΑΙ | | |
| 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 | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| εξουσιοδοτημένη τροποποίηση ή καταστροφής. | | | |
| | | | |
| **2.2. Ενημέρωση φορέα** | | | |
| | | | |
| **2.3. Παραδοτέα** | | | |
| • Αρχεία Τεκμηρίωσης | ΝΑΙ | | |
| • Αρχεία Δραστηριοτήτων Επεξεργασίας | ΝΑΙ | | |
| • Ανάλυση συμμόρφωσης ανά άρθρο του Κανονισμού. | ΝΑΙ | | |
| • Εκτίμηση αντικτύπου (Data Protection Impact Assessment) | ΝΑΙ | | |
| • Αποτίμηση Επικινδυνότητας (Risk Assessment) | ΝΑΙ | | |
| • Επικαιροποιημένα κείμενα πολιτικών GDRP | ΝΑΙ | | |
| | | | |
| **Φάση 3 - Επικαιροποίηση και κατάθεση σχεδίου δράσης συνεχούς συμμόρφωσης-** **Ενημέρωση** | | | |
| | | | |
| **3.1. Ενέργειες** | | | |
| **Εκπόνηση Σχεδίου Δράσης** | | | |
| Βάση της εκτίμησης επιπέδου συμμόρφωσης, την εκτίμηση αντικτύπου και την αποτίμηση επικινδυνότητας, ο ανάδοχος θα εκπονήσει και θα τεκμηριώσει σχέδιο δράσης για επικαιροποίηση της συμμόρφωσης 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 («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/επικαιροποίηση. | ΝΑΙ | | |
| 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. | ΝΑΙ | | |
| Ενδεικτικά τέτοιες αναφέρονται: | ΝΑΙ | | |
| • Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που πληροί τις νομικές απαιτήσεις και | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| αντιμετωπίζει το λειτουργικό κίνδυνο και τον κίνδυνο βλάβης των ατόμων | | | |
| • Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα των εργαζομένων | ΝΑΙ | | |
| • Κώδικας Δεοντολογίας που περιλαμβάνει άρθρα για την Προστασίας Δεδομένων Προσωπικού Χαρακτήρα | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για τη συλλογή και τη χρήση προσωπικών δεδομένων ειδικής κατηγορίας | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για τη συλλογή και χρήση των δεδομένων προσωπικού χαρακτήρα παιδιών και ανηλίκων | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για τη διατήρηση της ποιότητας των δεδομένων, | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για τη διαγραφή των προσωπικών δεδομένων, | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για τον έλεγχο της επεξεργασίας που διεξάγεται συνολικά ή εν μέρει με αυτοματοποιημένα μέσα | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για δευτερεύουσες χρήσεις των δεδομένων προσωπικού χαρακτήρα | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για την απόκτηση έγκυρης συναίνεσης | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για ασφαλή καταστροφή των δεδομένων | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για τη διατήρηση αρχείων | ΝΑΙ | | |
| • Πολιτική/διαδικασίες -όσον αφορά τα δεδομένα προσωπικού χαρακτήρα - για άμεση επικοινωνία, ηλεκτρονικό ταχυδρομείο κλπ | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε συμβόλαια συντήρηση και υποστήριξης | ΝΑΙ | | |
| • Πολιτική/διαδικασίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές πρόσληψης | ΝΑΙ | | |
| • Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ιστοσελίδα του Νοσοκομείου και στα μέσα κοινωνικής δικτύωσης | ΝΑΙ | | |
| • Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε πρακτικές υγείας και ασφάλειας | ΝΑΙ | | |
| • Οδηγίες για ενσωμάτωση της προστασίας των δεδομένων προσωπικού χαρακτήρα στις πρακτικές παρακολούθησης και αξιολόγησης των εργαζομένων, | ΝΑΙ | | |

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

| | | | |
|---|---|---|---|
| Επίσης θα πρέπει να αναπτυχθούν όλες οι απαραίτητες πολιτικές και διαδικασίες σε σχέση με τους συνεργάτες (προμηθευτές / συμβούλους / εταιρίες υποστήριξης κλπ) οι οποίες θα προστεθούν στα υπάρχοντα ή νέα συμβόλαια. Ενδεικτικά θα παραλαμβάνει | ΝΑΙ | | |
| • Απαιτήσεις από τους συνεργάτες για την προστασία των δεδομένων προσωπικού χαρακτήρα κατά την εκτέλεση συμβάσεων ή συμφωνιών, | ΝΑΙ | | |
| • Όροι για δέουσα επιμέλεια σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα | ΝΑΙ | | |
| • Δυνατότητα αξιολόγησης του κινδύνου που προέρχεται από τους συνεργάτες (right to audit) | ΝΑΙ | | |
| | ΝΑΙ | | |
| 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 της Φάσης 1. | ΝΑΙ | | |
| | ΝΑΙ | | |
| **Παρουσίαση του Σχεδίου Δράσης** | ΝΑΙ | | |
| Με την ολοκλήρωση του σχεδίου δράσης, ο ανάδοχος θα το παρουσιάσει μαζί με τα συμπεράσματα της ανάλυσής του, στην Διοίκηση και στα αρμόδια στελέχη του Νοσοκομείου Ο στόχος της παρουσίασης είναι να ενημερωθούν και να ευαισθητοποιηθούν όλα τα εμπλεκόμενα μέρη για το σχέδιο δράσης και τις απαιτήσεις του Κανονισμού και κυρίως για τις αλλαγές στις Πολιτικές / Διαδικασίες που αυτός επιφέρει. Με τον τρόπο αυτό θα διευκολυνθεί η λήψη των απαραίτητων διοικητικών αποφάσεων για την υλοποίηση των απαιτούμενων μέτρων/ενεργειών | ΝΑΙ | | |
| Ο Ανάδοχος θα πρέπει στην τελική διαμόρφωση/επικαιροποίηση του σχεδίου δράσης, και πριν την έγκριση του από την Διοίκηση, να λάβει υπόψη τις παρατηρήσεις και προτάσεις των στελεχών. Επίσης θα παρέχει τις ανάλογες υπηρεσίες υποστήριξης με την τεκμηρίωση της αναγκαιότητας των δράσεων. | ΝΑΙ | | |
| | | | |
| **3.2. Παραδοτέα** | | | |
| • Επικαιροποιημένο Σχέδιο Δράσης Συμμόρφωσης με τις απαραίτητες πολιτικές και διαδικασίες, ανά άρθρο του Κανονισμού. | ΝΑΙ | | |
| • Σχέδιο συνεχούς συμμόρφωσης-επικαιροποίησης με τον Κανονισμό | ΝΑΙ | | |
| • Παρουσίαση του σχεδίου δράσης | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| | | | |
| **Φάση 4 - Υλοποίηση του Σχεδίου Δράσης – Συνεχής Εκπαίδευση** | | | |
| | | | |
| **4.2 Ενέργειες** | | | |
| | | | |
| **Υλοποίηση του σχεδίου δράσης** | | | |
| Ο ανάδοχος, μετά την έγκριση από την Διοίκηση, έχει υποχρέωση να υλοποιήσει στο Σχέδιο Δράσης Συμμόρφωσης. Οι υποχρεώσεις του αναδόχου αφορούν τουλάχιστον: | ΝΑΙ | | |
| • Την υλοποίηση όλων των μέτρων/ενεργειών/διαδικασιών οι οποίες δεν απαιτούν την προμήθεια ή τροποποίηση εξοπλισμού/προγραμμάτων. | ΝΑΙ | | |
| • Την σύνταξη/επικαιροποίηση όλων των Πολιτικών/Διαδικασιών που απαιτούνται για την εναρμόνιση του Νοσοκομείου με τον Κανονισμό | ΝΑΙ | | |
| • Την παροχή υπηρεσιών συμβούλου στην υλοποίηση των μέτρων/ενεργειών που απαιτούν την προμήθεια ή τροποποίηση εξοπλισμού/προγραμμάτων. | ΝΑΙ | | |
| • Την εκπαίδευση του προσωπικού του Νοσοκομείου που εμπλέκονται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα. | ΝΑΙ | | |
| Ο ανάδοχος είναι υπεύθυνος για την υλοποίηση του σχεδίου δράσης. | ΝΑΙ | | |
| | | | |
| **Συνεχής Εκπαίδευση** | | | |
| Η σωστή εκπαίδευση του προσωπικού του Νοσοκομείου είναι κρίσιμη για την διαφύλαξη της ασφάλειας των δεδομένων προσωπικού χαρακτήρα. Για τον λόγο το προσωπικό του Νοσοκομείου θα πρέπει να εκπαιδευτεί κατάλληλα από τον ανάδοχο ώστε: | ΝΑΙ | | |
| • Να είναι ενήμερο για τον Κανονισμό, τις απαιτήσεις του και την υποχρέωση του Νοσοκομείου να συμμορφώνεται με αυτόν. | ΝΑΙ | | |
| • Να είναι γνώστες των Πολιτικών Προστασίας των δεδομένων προσωπικού χαρακτήρα καθώς και των διαδικασιών εφαρμογής τους και να τις αποδέχεται | ΝΑΙ | | |
| • Να καταλαβαίνει πλήρως το ρόλο και τις ευθύνες που του έχουν ανατεθεί σχετικά με τη συμμόρφωση με τον Κανονισμό, | ΝΑΙ | | |
| • Να γνωρίζουν λεπτομερώς τις διαδικασίες αντιμετώπισης συμβάντων αλλά και τις υπόλοιπες | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| 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: | ΝΑΙ | | |
| • Εκπαίδευση κατά την διάρκεια της εργασίας (on-the-job-training) | ΝΑΙ | | |
| • Μαζική εκπαίδευση | ΝΑΙ | | |
| • Εκπαιδευτικό και ενημερωτικό υλικό. | ΝΑΙ | | |
| | | | |
| **1.7. Παραδοτέα** | | | |
| • Τεκμηρίωση της υλοποίησης από τον ανάδοχο του Σχεδίου Δράσης. | ΝΑΙ | | |
| • Επικαιροποιημένες διαδικασίες και πολιτικές συμμόρφωσης με τον Κανονισμό. | ΝΑΙ | | |
| • Πρόγραμμα συνεχούς εκπαίδευσης και ενημέρωσης προσωπικού καθώς και σχετικό εκπαιδευτικό και ενημερωτικό υλικό | ΝΑΙ | | |
| | ΝΑΙ | | |
| **Φάση 5 – Επιθεώρηση Συμμόρφωσης – Παρουσίαση Αποτελεσμάτων** | | | |
| | | | |
| **5.1. Ενέργειες** | | | |
| Η διαδικασία συμμόρφωσης του Νοσοκομείου με τον Κανονισμό θα πρέπει να αποτελεί διαρκή και ανοιχτή δραστηριότητα τόσο του αναδόχου όσο και του Νοσοκομείου. Κατά τη φάση της επιθεώρησης συμμόρφωσης από τον ανάδοχο θα επιθεωρούνται 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 υπογραφεί, ώστε να επιβεβαιώνεται η διαφύλαξη της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων προσωπικού χαρακτήρα και των απαιτήσεων του Κανονισμού. | ΝΑΙ | | |
| Επιπλέον, θα επιθεωρούνται 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/Υποστήρικης που έχουν υπογραφεί με τους συνεργάτες, καθώς και το είδος της εκπαίδευσης / ενημέρωσης που έχουν λάβει, όσον αφορά την προστασία των | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| προσωπικών δεδομένων. | | | |
| Ορόσημα της διαδικασίας τοποθετούνται στο τέλος κάθε φάσης του έργου. Με την συμπλήρωση κάθε ορόσημου ο ανάδοχος θα πρέπει να επικαιροποιεί εάν απαιτείται κα τα παραδοτέα προηγούμενων φάσεων. | ΝΑΙ | | |
| | ΝΑΙ | | |
| Ο ανάδοχος αναλαμβάνει να εκτελέσει όποιο συμπληρωματικό μέτρο / ενέργεια προκύψει και στη συνέχεια να συντάξει τελική έκθεση με τα αποτελέσματα του εσωτερικού ελέγχου. | ΝΑΙ | | |
| Τα αποτελέσματα κάθε επιθεώρησης καταγράφονται και φυλάσσονται στο αρχείο του έργου τόσο από τον ανάδοχο όσο και από το Νοσοκομείο, αποτελούν δε περιουσιακό στοιχείο και του Νοσοκομείου. | ΝΑΙ | | |
| | | | |
| **Παρουσίαση Αποτελεσμάτων Επιθεώρησης Συμμόρφωσης** | | | |
| Ο ανάδοχος έχει υποχρέωση παρουσίασης προς τη Διοίκηση του Νοσοκομείου, των αποτελεσμάτων της επιθεώρησης συμμόρφωσης καθώς και του επικαιροποιημένου Data Protection Impact Assessment και Risk Assessment, με γραπτή έκθεση. Η Διοίκηση του Νοσοκομείου διατηρεί τη δυνατότητα να ζητήσει αυτοπρόσωπη παρουσίαση από τον ανάδοχο. | ΝΑΙ | | |
| | | | |
| **Τελική Επιθεώρηση υλοποίησης του έργου** | | | |
| Ο ανάδοχος υποχρεούται σε παρουσίαση προς τη Διοίκηση του Νοσοκομείου, της τελικής εικόνας πορείας του έργου, τρείς (3) μήνες πριν τη λήξη της σύμβασης. | ΝΑΙ | | |
| | | | |
| **5.3. Παραδοτέα** | | | |
| • Επικαιροποιημένο Αρχείο Τεκμηρίωσης | ΝΑΙ | | |
| • Επικαιροποιημένα Αρχεία Δραστηριοτήτων Επεξεργασίας | ΝΑΙ | | |
| • Επικαιροποιημένη Ανάλυση του επιπέδου συμμόρφωσης του Νοσοκομείου, ανά άρθρο του Κανονισμού. | ΝΑΙ | | |
| • Επικαιροποιημένη Εκτίμηση αντικτύπου (Data Protection Impact Assessment) | ΝΑΙ | | |
| • Επικαιροποιημένη Αποτίμηση Επικινδυνότητας (Risk Assessment) | ΝΑΙ | | |
| • Επικαιροποιημένο Σχέδιο Δράσης Συμμόρφωσης με τα συμπληρωματικά μέτρα και διαδικασίες, ανά άρθρο του Κανονισμού | ΝΑΙ | | |
| • Εκθέσεις επιθεωρήσεων | ΝΑΙ | | |

| | | | |
|---|---|---|---|
| • Τελική παρουσίαση αποτελεσμάτων του έργου | ΝΑΙ | | |
| | | | |
| | | | |
| **ΥΠΗΡΕΣΙΕΣ DPO** | | | |
| | | | |
| Ο ανάδοχος θα παρέχει στον Νοσοκομείο καθόλη τη διάρκεια της σύμβασης κατάλληλα καταρτισμένο και πιστοποιημένο άτομο προκειμένου να αναλάβει τα καθήκοντα του Data Protection Officer (DPO). Ο DPO θα πλαισιώνεται από κατάλληλη υποστηρικτική ομάδα, η οποία θα περιλαμβάνει κατ' ελάχιστο έναν Information Security Consultant, έναν IT Auditor και έναν Νομικό με εμπειρία πάνω σε θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων. | ΝΑΙ | | |
| 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 αντικτύπου (DPIA) και θα δημιουργεί καινούργιες για επεξεργασίες υψηλού ρίσκου. Ακόμα θα αναλαμβάνει την ενημέρωση του προσωπικού καθώς και τις εσωτερικές επιθεωρήσεις, με σκοπό την επίτευξη του βέλτιστου επιπέδου συμμόρφωσης. | ΝΑΙ | | |
| Η δραστηριότητα του DPO θα πρέπει να βρίσκεται σε συνεχή συντονισμό με την Ομάδα Έργου του Νοσοκομείου και το ΑΤΕΠΕΣΕ ως υπεύθυνης υπηρεσίας συντονισμού αυτής. | ΝΑΙ | | |
| | | | |
| **Άρθρο 3** | | | |
| **Χρονοδιάγραμμα Υλοποίησης** | | | |
| Το χρονοδιάγραμμα Υλοποίησης του έργου Συμμόρφωσης είναι 12 μήνες με προτεινόμενο χρόνο υλοποίησης ανά φάση: | ΝΑΙ | | |
| | | | |

| ΜΗΝΕΣ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Φάση 1 | X | X | X | | | | | | | | | |
| Φάση 2 | | X | X | X | | | | | | | | |
| Φάση 3 | | | X | X | X | | | | | | | |
| Φάση 4 | | | | | X | X | X | X | | | | |
| Φάση 5 | | | | | | | X | X | X | X | X | X |

| | | | |
|---|---|---|---|
| Υπηρεσίες DPO: X X X X X X X X X X X X | | | |
| | | | |
| **Προϋπολογισμός** | | | |
| | | | |
| 15.000€ πλέον ΦΠΑ. | ΝΑΙ | | |
| | | | |
| **Άρθρο 4** | | | |
| **Τεχνική και Επαγγελματική Ικανότητα αναδόχου** | | | |
| | | | |
| Ο ανάδοχος απαιτείται να | ΝΑΙ | | |
| • Έχει υλοποιήσει ή υλοποιεί τουλάχιστον πέντε (5) έργα GDPR | ΝΑΙ | | |
| • Να διαθέτει πιστοποίηση κατά ISO 9001 και ISO 27001 | ΝΑΙ | | |
| • Η προτεινόμενη δική του ομάδα έργου θα πρέπει να περιλαμβάνει κατ' ελάχιστο τις ακόλουθες ειδικότητες | ΝΑΙ | | |
| - Project Manager | ΝΑΙ | | |
| - Information Security Consultant | ΝΑΙ | | |
| - IT Auditor | ΝΑΙ | | |
| - Νομικό Σύμβουλο | ΝΑΙ | | |
| • Τα μέλη της ομάδας θα πρέπει να έχουν τουλάχιστον τουλάχιστον 5ετή εμπειρία σε θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων ενώ θα πρέπει να έχουν συμμετάσχει σε δύο (2) τουλάχιστον έργα με αντικείμενο θέματα ασφάλειας πληροφοριών/προσωπικών δεδομένων. | ΝΑΙ | | |
| • Ο Information Security Consultant, θα πρέπει να είναι πιστοποιημένος ISO 27001 auditors. | ΝΑΙ | | |
| Ένα μέλος της ομάδας θα πρέπει να διαθέτει βεβαίωση ως Data Protection Officer (DPO) από εταιρία πιστοποιήσεων ή αντίστοιχη βεβαίωση άλλου φορέα καθώς και εμπειρία με εμπειρία σε ανάλογη θέση φορέα Β΄ βάθμιας φροντίδας υγείας. | ΝΑΙ | | |