ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας
www.eopyy.gov.gr

Μαρούσι, 14/01/2021
Αρ. Πρωτ.: ΔΑ5Β/103/1

Γενική Δ/νση: Οικονομικών Υποθέσεων
Δ/νση: Προμηθειών
Τμήμα: Διαγωνιστικών Διαδικασιών
Πληροφορίες: Κ. Νικητάκης
Τηλ.: 210-8110972, Fax: 210-8110985
Ταχ. Δ/νση: Απ. Παύλου 12, Μαρούσι, 151 23
E-mail: d3.t2@eopyy.gov.gr

ΠΡΟΣΚΛΗΣΗ ΕΚΔΗΛΩΣΗΣ ΕΝΔΙΑΦΕΡΟΝΤΟΣ
Αριθ. 1/2021

ΘΕΜΑ: Πρόσκληση εκδήλωσης ενδιαφέροντος για τη σύναψη σύμβασης με αντικείμενο την ανάθεση των υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO) στο πλαίσιο εφαρμογής των κανόνων GDPR, σύμφωνα με το άρθρο 37 του 679/2019 Γενικού Κανονισμού της Ευρωπαϊκής Ένωσης και σύνταξη μελετών DPIA,με τη διαδικασία της απευθείας ανάθεσης, προϋπολογισθείσας δαπάνης 20.000,00€ μη συμπεριλαμβανομένου ΦΠΑ 24%.

Το Ν.Π.Δ.Δ. με την επωνυμία «**Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας »** με έδρα επί της οδού Απ. Παύλου 12, Μαρούσι, σύμφωνα με την αρ. 1717/735/23-12-2020 απόφαση του ΔΣ του ΕΟΠΥΥ και την ΑΑΥ Μ16/8-1-2021 σας προσκαλεί να εκδηλώσετε το ενδιαφέρον σας με την υποβολή προσφοράς για τη σύναψη σύμβασης με αντικείμενο την ανάθεση των υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO) στα πλαίσια εφαρμογής των κανόνων GDPR, σύμφωνα με το άρθρο 37 του 679/2019 Γενικού Κανονισμού της Ευρωπαϊκής Ένωσης και σύνταξη δύο (2) Μελετών Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA), με τη διαδικασία της απευθείας ανάθεσης, με τη διαδικασία της απευθείας ανάθεσης, προϋπολογισθείσας δαπάνης 20.000,00€ μη συμπεριλαμβανομένου ΦΠΑ 24%, η οποία θα βαρύνει τον ΚΑΕ 0419.

Κριτήριο για την επιλογή του Αναδόχου που θα αναλάβει την εν λόγω Σύμβαση και θα καλύπτει πλήρως τις ανάγκες της Υπηρεσίας, σύμφωνα με τις προδιαγραφές όπως αναλυτικά περιγράφονται στο παράρτημα Α (το οποίο αποτελεί αναπόσπαστο μέρος της παρούσας πρόσκλησης), είναι η **πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει τιμής**.

ΚΑΤΑΡΤΙΣΗ ΚΑΙ ΥΠΟΒΟΛΗ ΠΡΟΣΦΟΡΩΝ

Οι προσφορές υποβάλλονται στα Γραφεία της Κεντρικής Υπηρεσίας του Ε.Ο.Π.Υ.Υ., οδός Απ. Παύλου 12, Γενικό Πρωτόκολλο (Ισόγειο), μέσα σε **ενιαίο σφραγισμένο** φάκελο, μέχρι την **22/01/2021 ημέρα Παρασκευή και ώρα 15.00 π.μ.**. Προσφορά που υποβλήθηκε μετά την καθορισμένη ημερομηνία και ώρα, δεν θα λαμβάνεται υπόψη και θα επιστρέφεται στον ενδιαφερόμενο.
Στον φάκελο της προσφοράς θα πρέπει να αναγράφονται ευκρινώς τα παρακάτω:
α) Τα πλήρη στοιχεία του διαγωνιζόμενου (Επωνυμία, Διεύθυνση, αριθμός τηλεφώνου, φαξ, υπεύθυνος επικοινωνίας) **β)** «ΠΡΟΣΦΟΡΑ για τη « σύναψη σύμβασης με αντικείμενο την ανάθεση των υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO) στα πλαίσια

εφαρμογής των κανόνων GDPR, σύμφωνα με το άρθρο 37 του 679/2019 Γενικού Κανονισμού της Ευρωπαϊκής Ένωσης », **γ)** Θα αναγράφεται: «***Να μην ανοιχτεί, αλλά να παραδοθεί κλειστός στη Διεύθυνση Προμηθειών*** » και **δ)** Η ημερομηνία αποσφράγισης των προσφορών.

Στον φάκελο της προσφοράς, θα περιέχονται:

1. Νομιμοποιητικά στοιχεία του υποψήφιου Αναδόχου. Ενδεικτικά : ΦΕΚ ίδρυσης και τροποποιήσεις του (για ΑΕ & ΕΠΕ), αντίγραφο ή απόσπασμα του καταστατικού και των εγγράφων τροποποιήσεών του (για ΟΕ, ΕΕ, ΙΚΕ κλπ) και αντίγραφο της βεβαίωσης έναρξης επαγγέλματος για φυσικά πρόσωπα). Για την απόδειξη της νόμιμης σύστασης και εκπροσώπησης , στις περιπτώσεις που ο οικονομικός φορέας είναι νομικό πρόσωπο, προσκομίζει τα κατά περίπτωση νομιμοποιητικά έγγραφα σύστασης και νόμιμης εκπροσώπησης (όπως καταστατικά, πιστοποιητικά μεταβολών, αντίστοιχα ΦΕΚ, συγκρότηση Δ.Σ. σε σώμα, σε περίπτωση Α.Ε., κλπ., ανάλογα με τη νομική μορφή του διαγωνιζομένου). Από τα ανωτέρω έγγραφα πρέπει να προκύπτουν η νόμιμη σύστασή του, όλες οι σχετικές τροποποιήσεις των καταστατικών, το/τα πρόσωπο/α που δεσμεύει/ουν νόμιμα την εταιρία κατά την ημερομηνία διενέργειας του διαγωνισμού (νόμιμος εκπρόσωπος, δικαίωμα υπογραφής κλπ.), τυχόν τρίτοι, στους οποίους έχει χορηγηθεί εξουσία εκπροσώπησης, καθώς και η θητεία του/των ή/και των μελών του οργάνου διοίκησης/ νόμιμου εκπροσώπου.

2. Προσφορά σύμφωνα με όσα περιγράφονται στο παράρτημα Α, **που θα λαμβάνει υπόψη και τις εκεί αναφερόμενες προϋποθέσεις συμμετοχής**

Η τιμή προσφοράς δεν υπόκειται σε καμία αναπροσαρμογή ή αναθεώρηση, για οποιονδήποτε λόγο ή αιτία, θα ισχύει δε και θα δεσμεύει τον Ανάδοχο μέχρι την πλήρη εκτέλεση της προμήθειας. Η προσφορά θα φέρει υπογραφή και σφραγίδα του νόμιμου εκπροσώπου της εταιρείας. *Θα πρέπει να αναγράφεται το ονοματεπώνυμο του υπογράφοντος και σε περίπτωση εταιρείας να αποδεικνύεται με τα απαραίτητα έγγραφα ότι ο υπογράφων εκπροσωπεί νόμιμα την εταιρεία.*

Οι προσφορές θα ελεγχθούν την **25/01/2021 ημέρα Δευτέρα και ώρα 10.00π.μ.,** στη Δ/νση Προμηθειών, Τμήμα Διαγωνιστικών Διαδικασιών , Απ. Παύλου 12, Μαρούσι, στον 4ο όροφο, όπου μπορεί να παρευρεθεί όποιος ενδιαφερόμενος το επιθυμεί.

ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΔΕΙΞΗΣ ΜΕΙΟΔΟΤΗ - ΚΑΤΑΚΥΡΩΣΗ
Μετά την αξιολόγηση των προσφορών, ο προσφέρων στον οποίο πρόκειται να γίνει η κατακύρωση, εντός προθεσμίας δέκα (10) ημερών από τη σχετική ειδοποίηση που του αποστέλλεται, υποβάλλει σε σφραγισμένο φάκελο επί αποδείξει με σήμανση «Δικαιολογητικά Κατακύρωσης», τα κάτωθι δικαιολογητικά που απαιτούνται (άρθρο 80 Ν. 4412/16)

Α) Υπεύθυνη δήλωση εκ μέρους του οικονομικού φορέα, σε περίπτωση φυσικού προσώπου, ή σε περίπτωση νομικού προσώπου την υποβολή αυτής εκ μέρους του νομίμου εκπροσώπου, όπως αυτός ορίζεται στην περίπτωση 79Α του Ν.4412/16, ότι δεν έχουν καταδικαστεί με αμετάκλητη δικαστική απόφαση για τα αδικήματα που προβλέπονται στο άρθρο 73 παρ. 1 του Ν. 4412/2016, ΦΕΚ 147/Α/8-08-2016 όπως αυτός ισχύει και αδίκημα σχετικό με την άσκηση της επαγγελματικής τους δραστηριότητας.

Ως εκπρόσωπος του οικονομικού φορέα για την υποβολή της Υπεύθυνης Δήλωσης, νοείται ο νόμιμος εκπρόσωπος αυτού, όπως προκύπτει από το ισχύον καταστατικό ή το πρακτικό εκπροσώπησής του κατά το χρόνο υποβολής της προσφοράς ή αίτησης συμμετοχής ή το αρμοδίως εξουσιοδοτημένο φυσικό πρόσωπο να εκπροσωπεί τον οικονομικό φορέα για διαδικασίες σύναψης συμβάσεων ή για συγκεκριμένη διαδικασία σύναψης σύμβασης.

Β) Πιστοποιητικό που εκδίδεται από αρμόδια κατά περίπτωση αρχή, από το οποίο να προκύπτει ότι κατά την ημερομηνία προσκόμισής του είναι ενήμεροι **ως προς τις υποχρεώσεις τους που αφορούν τις εισφορές κοινωνικής ασφάλισης** (κυρίας και επικουρικής) και **ως προς τις φορολογικές τους υποχρεώσεις.**

Γ) Αποδεικτικά:

Στην περίπτωση που ο υποψήφιος είναι φυσικό πρόσωπο, θα πρέπει να διαθέτει κατ΄ ελάχιστο τα κάτωθι επαγγελματικά προσόντα:

i. *Πανεπιστημιακό πτυχίο ΑΕΙ νομικών επιστημών, ή σχολής πληροφορικής, ή σχολής μηχανικών πληροφορικής ή αντίστοιχο τίτλο σπουδών της αλλοδαπής αναγνωρισμένο από τον ΔΟΑΤΑΠ και άδεια άσκησης επαγγέλματος όπου απαιτείται*
ii. *Εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων.*
iii. *Αποδεδειγμένη νομική εμπειρία τουλάχιστον 3 ετών σε θέματα Προστασίας Προσωπικών Δεδομένων. Συνεκτιμάται η Πιστοποίηση από έγκριτο Φορέα της σχετικής Επάρκειας του ρόλου του Υπεύθυνου Προστασίας Δεδομένων (DPO)*

*Στην περίπτωση που ο υποψήφιος δηλώσει ότι πλαισιώνεται από συνεργάτες φυσικά πρόσωπα θα πρέπει κάθε μέλος της ομάδας έργου που ασκεί καθήκοντα υπευθύνου προστασίας δεδομένων να πληροί όλες τις ισχύουσες απαιτήσεις του ΓΚΠΔ **και τις ανωτέρω προϋποθέσεις**. Επιπρόσθετα:*

- *ένα (1) μέλος που θα ορισθεί ως ο υπεύθυνος του έργου (**PM**) εμπειρία τουλάχιστον 3 ετών στη Διαχείριση Έργων*
- *Το ένα (1) μέλος που θα είναι νομικός, ξεχωριστό φυσικό πρόσωπο από τον υπεύθυνο έργου, με αποδεδειγμένη νομική εμπειρία τουλάχιστον 3 ετών σε θέματα Προστασίας Προσωπικών Δεδομένων. Το μέλος αυτό που θα έχει το ρόλο του DPO, θα πρέπει να καλύπτει κατ΄ ελάχιστον τις απαιτήσεις ii έως iii της παρούσας παραγράφου 2 ανωτέρω. Συνεκτιμάται η Πιστοποίηση από έγκριτο φορέα της σχετικής επάρκειας του ρόλου του DPO*
- *δύο (2) μέλη θα πρέπει να έχουν αποδεδειγμένη εμπειρία σε θέματα Ασφάλειας Πληροφοριακών Συστημάτων και Πληροφοριών .*

Τα ανωτέρω θα τεκμαίρονται είτε από σχετικά πιστοποιητικά είτε από αποδεδειγμένη επαγγελματική εμπειρία (Συστατική επιστολή, Βεβαίωση καλής εκτέλεσης , κλπ)

Οι υποψήφιοι καλούνται να προσκομίσουν στοιχεία (τίτλοι σπουδών, εργασιακή εμπειρία, βεβαιώσεις, πιστοποιητικά), τα οποία θα αποδεικνύουν τα ανωτέρω.

Χρόνος Υλοποίησης

Η διάρκεια της σχετικής σύμβασης παροχής υπηρεσιών DPO ορίζεται σε χρονικό διάστημα 12 μηνών από την υπογραφή της, λύεται δε με την οριστική παραλαβή του έργου.

Πληρωμή (ν. 4412/2016 άρθρο 200 παρ.5)

Η πληρωμή της αξίας των ως άνω υπηρεσιών θα πραγματοποιηθεί τμηματικά, ανά τρίμηνο από την αρμόδια επιτροπή παραλαβής του Οργανισμού, μετά από προσκόμιση αναφοράς προόδου και πεπραγμένων, με χρηματικό ένταλμα που θα εκδοθεί στο όνομα της δικαιούχου αναδόχου, μετά την παραλαβή των άνωθι και σε χρόνο προσδιορισμένο από την αναγκαία διοικητική διαδικασία για έκδοση του σχετικού χρηματικού εντάλματος. Η Παροχή Υπηρεσιών DPO θα εξοφλείται σε 4 ισόποσες δόσεις ανά τρίμηνο, ενώ η σύνταξη των 2 μελετών DPIA, μετά την ολοκλήρωση και οριστική παραλαβή έκαστης.

Ο Ανάδοχος οφείλει να εκδίδει τα ανάλογα φορολογικά στοιχεία στα κάτωθι στοιχεία:
Επωνυμία :ΕΘΝΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ - (Ε.Ο.Π.Υ.Υ.)
Α.Φ.Μ. : 997478553

Δ.Ο.Υ. : Αμαρουσίου
Διεύθυνση : Απ. Παύλου 12
Τ.Κ. : 151 23 Μαρούσι

Ο Ανάδοχος βαρύνεται για συμβάσεις άνω των €2.500 που υπάγονται στο Ν. 4412/16 **α)** με τις νόμιμες κρατήσεις της παρ. 3 του άρθρου 4 του ν. 4013/2011, ήτοι 0,07% υπέρ της Ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων (επ' αυτού 3% χαρτοσήμου και επ' αυτού 20% ΟΓΑ χαρτοσήμου), **β)** με τις νόμιμες κρατήσεις του αρθρ. 350 παρ 3 του ν.4412/2016, ήτοι 0,06% υπέρ ΑΕΠΠ (επ' αυτού 3% χαρτοσήμου και επ' αυτού 20% ΟΓΑ χαρτοσήμου)

Με τις διατάξεις του άρθρου 64, του Ν. 4172/2013, στον ανάδοχο που θα αναδειχθεί επιβάλλεται παρακράτηση φόρου εισοδήματος, ο οποίος υπολογίζεται στο καθαρό ποσό της αξίας των αγαθών-υπηρεσιών.

Η συμμετοχή στη διαδικασία συνεπάγεται την χωρίς επιφύλαξη αποδοχή των όρων της παρούσας πρόσκλησης, οι βασικοί όροι της οποίας θα αποτελέσουν στοιχεία της σύμβασης και θα δεσμεύουν την επιχείρηση, στην περίπτωση που εκ παραλήψεως δεν θα περιληφθούν σε αυτή.

Ότι δεν αναγράφεται στην παρούσα πρόσκληση ρυθμίζεται σύμφωνα με τις διατάξεις του Ν.4412/2016.

Η Διοικήτρια ΕΟΠΥΥ

ΘΕΑΝΩ ΚΑΡΠΟΔΙΝΗ

ΠΑΡΑΡΤΗΜΑ Α – ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ – ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ

Στα πλαίσια της Εφαρμογής του Γενικού Κανονισμού της Ευρωπαϊκής Ένωσης 2016/679, ο οποίος θεσπίζει κανόνες που αφορούν στην Προστασία των Φυσικών Προσώπων, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα (General Data Protection Regulation –GDPR) , προκύπτει η υποχρέωση του ΕΟΠΥΥ, όπως και όλων των οργανισμών που επεξεργάζονται δεδομένα, να συμμορφώνονται με τις απαιτήσεις του Κανονισμού.
Σύμφωνα με το άρθρο 37 του Κανονισμού:
"..Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν υπεύθυνο προστασίας δεδομένων σε κάθε περίπτωση στην οποία:
α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας,
β) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή
γ) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.
2. Όμιλος επιχειρήσεων μπορεί να διορίσει ένα μόνο υπεύθυνο προστασίας δεδομένων, υπό την προϋπόθεση ότι κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων.
3. Εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσια αρχή ή δημόσιος φορέας, ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές τέτοιες αρχές ή πολλούς τέτοιους φορείς, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους.
4. Σε περιπτώσεις πλην των αναφερόμενων στην παράγραφο 1, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να ορίζουν υπεύθυνο προστασίας δεδομένων ή, όπου απαιτείται από το δίκαιο της Ένωσης ή του κράτους μέλους, ορίζουν υπεύθυνο προστασίας δεδομένων. Ο υπεύθυνος προστασίας δεδομένων μπορεί να ενεργεί για τις εν λόγω ενώσεις και τους άλλους φορείς που εκπροσωπούν υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία.
5. Ο υπεύθυνος προστασίας δεδομένων διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39.
6. Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών.
7. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δημοσιεύουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και τα ανακοινώνουν στην εποπτική αρχή…"

1. ΑΝΑΓΚΑΙΟΤΗΤΑ ΑΜΕΣΟΥ ΔΙΟΡΙΣΜΟΥ DPO

Λαμβάνοντας υπόψη:

- ✓ Τα αναφερόμενα στο άρθρο 37, όπως αναλύονται ανωτέρω
- ✓ *Την αναγκαιότητα παροχής υπηρεσιών Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO στα πλαίσια εφαρμογής των κανόνων GDPR, σύμφωνα με το άρθρο 37 του 679/2016 Γενικού Κανονισμού της Ευρωπαϊκής Ένωσης, στα πλαίσια της υπο-*

χρέωσης του ΕΟΠΥΥ, όπως και όλων των οργανισμών που επεξεργάζονται δεδομένα, να συμμορφώνονται με τις απαιτήσεις του Κανονισμού.

- ✓ Το γεγονός ότι η μη συμμόρφωση με τις διατάξεις του 2016/679 , επιφέρει ,σύμφωνα με το άρθρο 83, αυστηρές κυρώσεις στον εκτελών την επεξεργασία, κρίνεται σκόπιμη η ανάθεση των υπηρεσιών του Υπευθύνου Προστασίας σε εξωτερικό συνεργάτη με σχετική Σύμβαση Έργου

2. ΑΝΤΙΚΕΙΜΕΝΟ

Αντικείμενο του έργου αποτελεί:

Α. Η ανάθεση των υπηρεσιών του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer – DPO) στα πλαίσια εφαρμογής των κανόνων GDPR, σύμφωνα με το άρθρο 37 του 679/2016 Γενικού Κανονισμού της Ευρωπαϊκής Ένωσης. Ο Κανονισμός (ΕΕ) αριθ. 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και της ελεύθερης κυκλοφορίας των δεδομένων αυτών (γνωστός και ως «κανονισμός γενικής προστασίας δεδομένων» ή «GDPR»)έχει τεθεί σε ισχύ σε ολόκληρη την ΕΕ στις 25 Μαΐου 2018. Στις 29 Αυγούστου του 2019 εκδόθηκε και ο Ν.4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων».

Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ) - Σύμφωνα με το άρθρο 37 παράγραφος 1 του GDPR, ο διορισμός ενός ΥΠΔ είναι υποχρεωτικός όταν:

- η σχετική δραστηριότητα επεξεργασίας δεδομένων διεξάγεται από δημόσια αρχή ή οργανισμό
- οι κύριες δραστηριότητες του Οργανισμού περιλαμβάνουν τακτική και συστηματική παρακολούθηση των ατόμων, σε μεγάλη κλίμακα
- οι βασικές δραστηριότητες του Οργανισμού περιλαμβάνουν τη διεκπεραίωση σε ευρεία κλίμακα ευαίσθητων προσωπικών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα
- το απαιτεί το εθνικό δίκαιο.

Αυτό εξηγείται λεπτομερέστερα στις κατευθυντήριες γραμμές που δημοσίευσε η ομάδα εργασίας του άρθρου 29 (Guidelines On Data Protection Officers ('Dpos') - Article 29 Data Protection Working Party – 13.12.2016).

Καθήκοντα - Δραστηριότητες του Υπευθύνου Προστασίας Δεδομένων (DPO)

Σύμφωνα με το άρθρο 39 παράγραφος 1, τα κύρια καθήκοντα και οι δραστηριότητες του ΥΠΔ είναι:

- να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας και τους εργαζόμενους που διεκπεραιώνουν τις υποχρεώσεις τους βάσει του GDPR και άλλων εφαρμοστέων νόμων και κανονισμών της ΕΕ,
- να παρακολουθεί τη συμμόρφωση με το GDPR κλπ., καθώς και με τις πολιτικές του υπεύθυνου επεξεργασίας όσον αφορά στην προστασία των προσωπικών δεδομένων, συμπεριλαμβανομένης της ανάθεσης ευθυνών, της ευαισθητοποίησης και της κατάρτισης του προσωπικού που εμπλέκεται στις εργασίες επεξεργασίας, καθώς και των συναφών ελέγχων
- να παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση των επιπτώσεων στην προστασία δεδομένων και να παρακολουθεί την απόδοσή της σύμφωνα με το άρθρο 35, •
- να συνεργάζεται με την εποπτική αρχή και
- να ενεργεί ως σημείο επαφής της εποπτικής αρχής σε θέματα που αφορούν την επεξεργασία κ.λπ.

- «να λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις εργασίες επεξεργασίας, λαμβανομένης υπόψη της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας» (βλ. Άρθρο 39 παράγραφος 2).
- *εκπόνηση δύο (2) Μ.Ε.Α. σχετικά με την Προστασία Δεδομένων (DPIA) κατόπιν σχετικής απαίτησης από τον ΕΟΠΥΥ*

Σύμφωνα με την οδηγία για το ρόλο του DPO (Guidelines On Data Protection Officers ('Dpos') - Article 29 Data Protection Working Party – 13.12.2016), οι ΥΠΔ πρέπει να διαθέτουν τις κατάλληλες επαγγελματικές ικανότητες και εξειδικευμένες γνώσεις σχετικά με τις επιχειρησιακές διαδικασίες του οργανισμού, των μέσων ελέγχου συμμόρφωσης και τη νομοθεσία περί προστασίας των δεδομένων.
Οι δραστηριότητες περίπλοκων ή υψηλού κινδύνου επεξεργασίας δεδομένων θα απαιτήσουν από τον ΥΠΔ να έχει μεγαλύτερη εμπειρογνωμοσύνη.
Σύμφωνα με την οδηγία, ο ΥΠΔ θα πρέπει, ιδανικά, να βρίσκεται εντός της ΕΕ για να διασφαλίσει ότι ο ΥΠΔ είναι προσβάσιμος στον οργανισμό. Επιπλέον, συνιστάται στους οργανισμούς να διατηρούν ένα γραπτό αντίγραφο των αποφάσεων που οδηγούν στον διορισμό του ΥΠΔ (στο πλαίσιο των ευρύτερων υποχρεώσεών τους για λογοδοσία).
Ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ) διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και των εκτελούντων την επεξεργασία προς τις διατάξεις του ΓΚΠΔ και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός). Καταρχήν δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση προς τον ΓΚΠΔ, έχει όμως βέβαια την ευθύνη καθοδήγησης του φορέα προς την απαιτούμενη συμμόρφωση προς το ΓΚΠΔ. (Επισημαίνεται ότι υπεύθυνος πρέπει να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία).

Συγκεκριμένα ο ανάδοχος:

- Εκτελεί όλα τα καθήκοντα του ΥΠΔ (DPO) , είναι προσβάσιμος από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, αλλά και από τα υποκείμενα των δεδομένων 24ώρες το 24ωρο και 365 ημέρες το χρόνο.
- Ενημερώνει και συμβουλεύει τη Διοικητική Ομάδα του Οργανισμού, τους υπεύθυνους επικοινωνίας και τους υπαλλήλους που επεξεργάζονται ή εμπλέκονται με οποιονδήποτε τρόπο στην διαχείριση δεδομένων προσωπικού χαρακτήρα αναφορικά με τις υποχρεώσεις τους που απορρέουν από την Ευρωπαϊκή και την Εθνική Νομοθεσία σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα
- Καθοδηγεί για την εφαρμογή των κατάλληλων μέτρων και για την απόδειξη της συμμόρφωσης, ιδίως όσον αφορά τον προσδιορισμό των κινδύνων που συνδέονται με την επεξεργασία, την εκτίμηση τους από άποψη προέλευσης, φύσης, πιθανότητας και σοβαρότητας και τον εντοπισμό των βέλτιστων πρακτικών για τον περιορισμό των κινδύνων
- Παρακολουθεί τη συμμόρφωση με τη νομοθεσία σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της πρότασης αναμόρφωσης των διαδικασιών, της επικαιροποίησης της χαρτογράφησης δεδομένων και ροών, της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και της διενέργειας σχετικών ελέγχων
- Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντίκτυπου σχετικά με την προστασία των δεδομένων και θα παρακολουθεί την υλοποίηση της σύμφωνα με το άρθρο 35 του Κανονισμού
- Συμμετέχει, δεόντως και εγκαίρως, στη διαδικασία λήψης αποφάσεων για τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.
- Είναι διαθέσιμος παρέχοντας διασφάλιση της δυνατότητας επικοινωνίας των υποκειμένων των δεδομένων μαζί του για κάθε ζήτημα σχετικά με την επεξεργασία των δεδομένων και την άσκηση των δικαιωμάτων τους. Η διαθεσιμότητα του δύναται να εξασφαλισθεί είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας.

- Έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας και εγκαταστάσεις σχετικών υποδομών, εφόσον κρίνεται απολύτως απαραίτητη, με σκοπό την ορθή ενάσκηση των καθηκόντων του.
- Διατυπώνει όλες τις απαντήσεις, προτάσεις, ενημερώσεις, οδηγίες, συμβουλές του ΥΠΔ προς τον Οργανισμό.
- Έχει φυσική παρουσία στον Οργανισμό ώστε να παρακολουθεί και να υπογραμμίζει πιθανές αστοχίες από τους εμπλεκόμενους υπαλλήλους στο σχέδιο που θα καταρτιστεί για την εφαρμογή της συμμόρφωσης.
- Αξιοποιεί και επικαιροποιεί τις υπάρχουσες καταγραφές των ροών, διαδικασιών, συστημάτων και προσώπων που προβαίνουν σε επεξεργασία προσωπικών δεδομένων
- Διαχειρίζεται και μειώνει τους κινδύνους από την επεξεργασία και αποκλίσεων από τις επιταγές του Κανονισμού.
- Καταγράφει τις ανάγκες.
- Παρακολουθεί την εσωτερική συμμόρφωση με τον ΓΚΠΔ και άλλες διατάξεις περί προστασίας δεδομένων (π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).
- Συνεργάζεται με την εποπτική αρχή και ενεργεί ως σημείο επικοινωνίας με την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της διαβούλευσης που αναφέρεται στο άρθρο 36 του ΓΚΠΔ.
- Προσδιορίζει τις νομικές βάσεις επεξεργασίας προσωπικών δεδομένων, συμπεριλαμβανομένης της συναίνεσης του υποκειμένου.
- Εισηγείται και ελέγχει τις διατυπώσεις σε συμβάσεις, έντυπα ενημέρωσης και χορήγησης συγκατάθεσης.
- Είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, ασθενείς, κ.λπ.).
- Υποστηρίζει στη Διαχείριση Αιτημάτων και Παραβιάσεων.
- Αναπτύσσει σχέδιο απόκρισης για την παραβίαση δεδομένων και προετοιμασία πρωτοκόλλου γνωστοποίησης παραβίασης στην εποπτεύουσα αρχή και σχετικής ανακοίνωσης στα υποκείμενα.
- Προτείνει τη διαμόρφωση οργανωτικών και τεχνικών μέτρων και ανάπτυξη και υλοποίηση πρότυπων έγγραφων διαδικασιών.
- Συνεργάζεται με τη Διοίκηση και τα αρμόδια στελέχη για την επικαιροποίηση Πολιτικών Ασφαλείας και Διαδικασιών.
- Προβαίνει σε ενημέρωση του Οργανισμού για οποιαδήποτε νέα σχετική απαίτηση της Νομοθεσίας σχετικά με την προστασία ΔΠΧ. Ακόμα, ενημερώνει συνολικά για τις εξελίξεις γύρω από το χώρο του GDPR προκειμένου ο Οργανισμός να βρίσκεται πάντοτε σε πλεονεκτική θέση και να κατέχει σημαντικό ανταγωνιστικό πλεονέκτημα, που θα τον κάνει στο τέλος και να ξεχωρίζει.
- 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 ΕΟΠΥΥ, ενώ παράλληλα δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του.
- Η σύνταξη δύο (2) Μελετών Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA) κατόπιν σχετικής απαίτησης από τον ΕΟΠΥΥ

Β. Μελέτη Εκτίμησης Αντικτύπου (DPIA)

Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών τέθηκε σε ισχύ στις 25 Μαΐου 2018. Ο ΓΚΠΔ περιέχει ένα αναθεωρημένο σύστημα προστασίας των δεδομένων προσωπικού χαρακτήρα στην ΕΕ, το οποίο αποσκοπεί στη διασφάλιση υψηλού επιπέδου προστασίας των φυσικών προσώπων (υποκειμένων) με συνεκτική και ομοιόμορφη εφαρμογή των κανόνων για την προστασία των θεμελιωδών δικαιωμάτων και των ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την Ένωση.
Για τους σκοπούς αυτούς, ο ΓΚΠΔ χαρακτηρίζεται, ιδίως, από την ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων και την αντίστοιχη επαύξηση των υποχρεώσεων και των ευθυνών των υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία, οι οποίοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα εντός της ΕΕ.
Η υποχρέωση διενέργειας Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA), που βαρύνει πλέον ρητά τον υπεύθυνο επεξεργασίας με βάσει τις διατάξεις του ΓΚΠΔ, παρίσταται, ταυτόχρονα, ως ένα σημαντικό μέτρο προστασίας των υποκειμένων των δεδομένων από «υψηλούς κινδύνους» και ως ένα εξίσου σημαντικό μέτρο συμμόρφωσης των υπεύθυνων επεξεργασίας προς τις διατάξεις του ΓΚΠΔ.
Η ρητή θέσπιση υποχρέωσης διενέργειας DPIA παρίσταται, καταρχάς, ως αντιστάθμισμα στην κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας, με σκοπό την αντιμετώπιση των υψηλών κινδύνων, που ενδέχεται να προκύψουν για τα υποκείμενα των δεδομένων από συγκεκριμένες κατηγορίες επεξεργασιών, λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους. Ωστόσο, η υποχρέωση διενέργειας DPIA θεσπίζεται στο ΓΚΠΔ κυρίως ως ένα μέτρο ενίσχυσης της συμμόρφωσης προς τις διατάξεις του, λαμβανομένης πάντοτε υπόψη της ανάγκης αντιμετώπισης των υψηλών κινδύνων, που ενδέχεται να προκύψουν για τα υποκείμενα των δεδομένων από συγκεκριμένες κατηγορίες επεξεργασιών, λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους.
Υπό την έννοια αυτή η υποχρέωση διενέργειας DPIA σημαίνει ότι ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να αξιολογήσει όλες τις παραμέτρους των κρίσιμων πράξεων επεξεργασίας πριν από την έναρξή τους, προκειμένου να διασφαλίσει την αποτελεσματική προστασία των υποκειμένων. Επιπλέον, εάν απαιτείται από τις περιστάσεις, ο υπεύθυνος επεξεργασίας υποχρεούται να πραγματοποιεί σχετικά διαβούλευση με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), πριν από την έναρξη της επεξεργασίας.
Συνακόλουθα, η υποχρέωση διενέργειας DPIA σημαίνει, επίσης, ότι πρόκειται για ένα μέτρο, το οποίο είναι πλήρως ενταγμένο στην ανάγκη προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (Privacy by Design/Privacy by Default), σύμφωνα με τα οριζόμενα στις διατάξεις του άρθρου 25 του ΓΚΔΠ.
Ο υπεύθυνος επεξεργασίας υποχρεούται ρητά σε διενέργεια DPIA, πριν από την κρίσιμη επεξεργασία, κάθε φορά που ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών, και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας αυτής, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Είναι δυνατόν η διενέργεια DPIA να μην αφορά μεμονωμένη επεξεργασία, αλλά ένα σύνολο πράξεων επεξεργασίας, εφόσον αυτές είναι παρόμοιες και ενέχουν παρόμοιους υψηλούς κινδύνους για τα ενδιαφερόμενα υποκείμενα.
Ο ΓΚΠΔ, εξειδικεύοντας την έννοια των επεξεργασιών δυνάμενων να επιφέρουν ως άνω υψηλούς κινδύνους καθιστά τη διενέργεια DPIA υποχρεωτική σε τρεις τουλάχιστον τύπους επεξεργασιών:

- της συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών των υποκειμένων, που βασίζεται σε αυτοματοποιημένη επεξεργασία (συμπεριλαμβανομένης της τεχνικής profiling) και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα για τα υποκείμενα αυτά ή τα επηρεάζουν σε σημαντικό βαθμό,
- της μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9§1 ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέ-

ρονται στο άρθρο 10 (δηλαδή, σχετικών με ευαίσθητα δεδομένα προσωπικού χαρακτήρα),
- της συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Πέρα από τους ως άνω τύπους επεξεργασιών που προσδιορίζονται ρητά, θεσπίζεται υποχρέωση της ΑΠΔΠΧ να καταρτίζει και να δημοσιοποιεί κατάλογο με τους τύπους επεξεργασίας, που υπόκεινται -κατά την κρίση της- στην υποχρέωση για διενέργεια DPIA. Θεσπίζεται, επίσης, ευχέρεια της ΑΠΔΠΧ να καταρτίζει και να δημοσιοποιεί κατάλογο με τους τύπους επεξεργασίας, που εξαιρούνται από την υποχρέωση για διενέργεια DPIA. Τόσο ο κατάλογος, με τους τύπους επεξεργασίας για τους οποίους απαιτείται η διενέργεια DPIA, όσο και ο κατάλογος με εκείνους που εξαιρούνται από τη διενέργεια DPIA, ανακοινώνονται από την αρμόδια ΑΠΔΠΧ στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων.

Το περιεχόμενο της DPIA, που διενεργείται υποχρεωτικά κατά τα προαναφερόμενα, σύμφωνα με το ΓΚΠΔ συνίσταται σε:
- συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών αυτών, καθώς και του εννόμου συμφέροντος που επιδιώκει, κατά περίπτωση, ο υπεύθυνος επεξεργασίας,
- εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς τους,
- εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων,
- τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς το ΓΚΠΔ, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα τόσο των υποκειμένων των δεδομένων όσο και άλλων ενδιαφερόμενων προσώπων.

Εφόσον υπάρχει εκτελών την επεξεργασία, πρέπει να παρέχει συνδρομή στον υπεύθυνο επεξεργασίας, όταν χρειάζεται και αφού του ζητηθεί, ώστε να διασφαλίζει τη συμμόρφωση προς τις υποχρεώσεις, που απορρέουν από τη διενέργεια DPIA, σχετικά με την προστασία των δεδομένων, και από την προηγούμενη διαβούλευση με την αρμόδια ΑΠΔΠΧ.

ΜΕΘΟΔΟΛΟΓΙΑ DPIA

Κατά την εκτίμηση του αντικτύπου μιας πράξης επεξεργασίας δεδομένων πρέπει να λαμβάνεται υπόψη (άρθρο 35 § 8 ΓΚΠΔ) η συμμόρφωση με έναν κώδικα δεοντολογίας (άρθρο 40 ΓΚΠΔ). Τούτο μπορεί επίσης να χρησιμεύσει στην απόδειξη ότι έχουν επιλεγεί ή ληφθεί τα κατάλληλα μέτρα, με τον όρο ότι ο κώδικας δεοντολογίας ενδείκνυται για την πράξη επεξεργασίας. Πρέπει επίσης να λαμβάνονται υπόψη οι πιστοποιήσεις, οι σφραγίδες και τα σήματα [προστασίας των δεδομένων] για τον σκοπό της απόδειξης της συμμόρφωσης των πράξεων επεξεργασίας των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία (άρθρο 42 ΓΚΠΔ) με τον ΓΚΠΔ, καθώς και οι δεσμευτικοί εταιρικοί κανόνες.

Όλες οι συναφείς απαιτήσεις που περιέχει ο ΓΚΠΔ παρέχουν ένα ευρύ, γενικό πλαίσιο για τον σχεδιασμό και την υλοποίηση DPIA. Η πρακτική υλοποίηση μιας DPIA θα εξαρτηθεί από την πλήρωση των απαιτήσεων του ΓΚΠΔ, οι οποίες μπορεί να συμπληρωθούν με πιο αναλυτικές πρακτικές οδηγίες. Ως εκ τούτου, η υλοποίηση DPIA είναι κλιμακούμενη. Τούτο σημαίνει ότι ακόμη και ένας μικρής εμβέλειας υπεύθυνος επεξεργασίας μπορεί να σχεδιάσει και να διενεργήσει DPIA πρόσφορη για τις πράξεις επεξεργασίας του.

Η αιτιολογική σκέψη 90 του ΓΚΠΔ παραθέτει μια σειρά στοιχείων της DPIA που αλληλεπικαλύπτονται με τα πλήρως καθορισμένα στοιχεία της διαχείρισης κινδύνων (λ.χ. ISO 31000). Με όρους διαχείρισης κινδύνου, μια DPIA αποσκοπεί στη «διαχείριση των κινδύνων» για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, με χρήση των ακόλουθων διαδικασιών, μέσω:
- του καθορισμού του πλαισίου: «λαμβάνοντας υπόψη τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας και τις πηγές του κινδύνου»,

- της εκτίμησης των κινδύνων: «ώστε να εκτιμήσει την ιδιαίτερη πιθανότητα και τη σοβαρότητα του υψηλού κινδύνου»,
- της αντιμετώπισης των κινδύνων: «που μετριάζουν αυτόν τον κίνδυνο» και «διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα» και «αποδεικνύουν τη συμμόρφωση προς τον παρόντα κανονισμό».

Ο ΓΚΠΔ παρέχει ευελιξία στους υπεύθυνους επεξεργασίας για τον καθορισμό της ακριβούς δομής και της μορφής της DPIA, προκειμένου αυτή να εξυπηρετεί τις υφιστάμενες πρακτικές εργασίας. Υπάρχουν πολυάριθμες καθιερωμένες διαδικασίες, εντός της ΕΕ και παγκοσμίως, που λαμβάνουν υπόψη τα στοιχεία που περιγράφονται στην αιτιολογική σκέψη 90. Ωστόσο, ανεξαρτήτως της μορφής που θα λάβει, η DPIA πρέπει να αποτελεί μια πραγματική αξιολόγηση των κινδύνων, που θα παρέχει στους υπεύθυνους επεξεργασίας τη δυνατότητα να λάβουν μέτρα για την αντιμετώπισή τους.

Διαφορετικές μεθοδολογίες θα μπορούσαν να χρησιμοποιηθούν για να συνδράμουν στην υλοποίηση των βασικών απαιτήσεων που θέτει ο ΓΚΠΔ. Έχουν προσδιοριστεί ορισμένα κοινά κριτήρια ώστε να επιτρέπεται στους υπεύθυνους επεξεργασίας να υιοθετούν διαφορετικές προσεγγίσεις, συμμορφούμενοι παράλληλα με τον ΓΚΠΔ. Τα εν λόγω κριτήρια αποσαφηνίζουν τις βασικές απαιτήσεις του Κανονισμού και παρέχουν επαρκές έδαφος για τη χρήση διαφορετικών μορφών υλοποίησης. Τα εν λόγω κριτήρια μπορούν να χρησιμοποιηθούν για την απόδειξη ότι μια συγκεκριμένη μεθοδολογία DPIA πληροί τα απαιτούμενα πρότυπα που θέτει ο ΓΚΠΔ. Ο υπεύθυνος επεξεργασίας είναι αρμόδιος να επιλέξει τη μεθοδολογία.

Τέλος, όποτε απαιτείται, «ο υπεύθυνος επεξεργασίας προβαίνει σε επανεξέταση για να εκτιμήσει εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διενεργείται σύμφωνα με την εκτίμηση αντικτύπου στην προστασία δεδομένων τουλάχιστον όταν μεταβάλλεται ο κίνδυνος που θέτουν οι πράξεις επεξεργασίας» (άρθρο 35§11).

3. ΠΡΟΫΠΟΘΕΣΕΙΣ ΣΥΜΜΕΤΟΧΗΣ:

Στην περίπτωση που ο υποψήφιος είναι φυσικό πρόσωπο, θα πρέπει να διαθέτει κατ' ελάχιστο τα κάτωθι επαγγελματικά προσόντα:

i. Πανεπιστημιακό πτυχίο ΑΕΙ νομικών επιστημών, ή σχολής πληροφορικής, ή σχολής μηχανικών πληροφορικής ή αντίστοιχο τίτλο σπουδών της αλλοδαπής αναγνωρισμένο από τον ΔΟΑΤΑΠ και άδεια άσκησης επαγγέλματος όπου απαιτείται
ii. Εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων.
iii. αποδεδειγμένη νομική εμπειρία τουλάχιστον 3 ετών σε θέματα Προστασίας Προσωπικών Δεδομένων. Συνεκτιμάται η Πιστοποίηση από έγκριτο φορέα της σχετικής επάρκειας του ρόλου του DPO.

Στην περίπτωση που ο υποψήφιος δηλώσει ότι πλαισιώνεται από συνεργάτες φυσικά πρόσωπα θα πρέπει κάθε μέλος της ομάδας έργου που ασκεί καθήκοντα υπευθύνου προστασίας δεδομένων να πληροί όλες τις ισχύουσες απαιτήσεις του ΓΚΠΔ και τις ανωτέρω προϋποθέσεις. Για λόγους νομικής σαφήνειας, καλής οργάνωσης και αποφυγής των συγκρούσεων συμφερόντων για τα μέλη της ομάδας, θα πρέπει στην αίτηση του υποψηφίου (στην τεχνική προσφορά) να υπάρχει σαφής καταμερισμός των καθηκόντων στα φυσικά πρόσωπα που θα δηλώσει και να ορίζεται ένα μόνο άτομο ως επικεφαλής επικοινωνίας και υπεύθυνος. Συγκεκριμένα στην Ομάδα Έργου θα πρέπει να εμφανίζονται κατ' ελάχιστο:

- ένα (1) μέλος θα ορισθεί ως ο υπεύθυνος του έργου (**PM**) εμπειρία τουλάχιστον 3 ετών στη Διαχείριση Έργων
- Το ένα (1) μέλος που θα είναι νομικός, ξεχωριστό φυσικό πρόσωπο από τον υπεύθυνο έργου, με αποδεδειγμένη νομική εμπειρία τουλάχιστον 3 ετών σε θέματα Προστασίας Προσωπικών Δεδομένων. Το μέλος αυτό που θα έχει το ρόλο του DPO, θα πρέπει να καλύπτει κατ΄ ελάχιστον τις απαιτήσεις i έως iii της παρούσας παραγράφου 2 ανωτέρω. Συνεκτιμάται η Πιστοποίηση από έγκριτο φορέα της σχετικής επάρκειας του ρόλου του DPO

- δύο (2) μέλη θα πρέπει να έχουν αποδεδειγμένη εμπειρία σε θέματα Ασφάλειας Πληροφοριακών Συστημάτων και Πληροφοριών .

Φυσική παρουσία: Ο συμβασιούχος (και η τυχόν οργανωμένη ομάδα αυτού) που θα επιλεγεί και θα υπογράψει σύμβαση, θα παρέχει τις υπηρεσίες του εντός και εκτός των χώρων του ΕΟΠΥΥ. Ο ΥΠΔ υποχρεούται να πραγματοποιεί τουλάχιστον 10 επισκέψεις μηνιαίως στα γραφεία του ΕΟΠΥΥ για την άσκηση των καθηκόντων του, διάρκειας όχι μικρότερης των 6 πλήρων ωρών (εκάστης) σε πρωινή και εργάσιμη ώρα και να παρέχει συμβουλές τηλεφωνικά ή μέσω ηλεκτρονικού ταχυδρομείου όποτε αυτό ζητηθεί. Οι ημέρες και ώρες των επισκέψεων θα οριστούν σε συνεργασία με την Αναθέτουσα Αρχή

Τα ανωτέρω θα τεκμαίρονται είτε από σχετικά πιστοποιητικά είτε από αποδεδειγμένη επαγγελματική εμπειρία (Συστατική επιστολή, Βεβαίωση καλής εκτέλεσης , κλπ)

Οι υποψήφιοι καλούνται να προσκομίσουν στοιχεία (τίτλοι σπουδών, εργασιακή εμπειρία, βεβαιώσεις, πιστοποιητικά), τα οποία θα αποδεικνύουν τα ανωτέρω.

4. ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ ΥΛΟΠΟΙΗΣΗΣ ΤΟΥ ΕΡΓΟΥ

Ο χρόνος ανάθεσης καθηκόντων DPO και μελετών DPIA ορίζεται σε **ένα (1) έτος** από την υπογραφή της σχετικής σύμβασης.

5. ΕΝΤΥΠΟ ΥΠΟΒΟΛΗΣ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ

Α/Α	***ΠΕΡΙΓΡΑΦΗ***	***Ποσότητα***	***Τιμή Μονάδος (€) χωρίς ΦΠΑ***	***Σύνολα (€) χωρίς ΦΠΑ***
1	***Παροχή Υπηρεσιών DPO***	***1***		
2	***Σύνταξη Μελέτης Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA) κατόπιν σχετικής απαίτησης από τον ΕΟΠΥΥ***	***2***		
			ΣΥΝΟΛΟ :	
			ΦΠΑ (24%):	
			ΓΕΝΙΚΟ ΣΥΝΟΛΟ (ΣΥΜΠ/ΝΟΥ ΦΠΑ)	