**ΜΕΡΟΣ Α - ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΒΑΣΗΣ**

**Αντικείμενο της Διακήρυξης**

Αντικείμενο της Διακήρυξης είναι η ανάδειξη Αναδόχου Παροχής Υπηρεσίας στα πλαίσια υλοποίησης της Πράξης με τίτλο «Δράσεις υποστήριξης της λειτουργίας του Ειδικού Λογαριασμού Κονδυλίων Έρευνας του Πανεπιστημίου Ιωαννίνων, ως δικαιούχου στη διαχείριση και υλοποίηση παρεμβάσεων του ΕΠΑΝΑΔΕΔΒΜ», Υποέργο 3 «ΠΡΟΣΑΡΜΟΓΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ / ΥΠΟΣΥΣΤΗΜΑΤΩΝ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΙΩΑΝΝΙΝΩΝ ΚΑΙ ΤΟΥ ΕΛΚΕ, ΣΤΟ ΝΕΟ ΚΑΝΟΝΙΣΜΟ ΓΙΑ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ», με κωδικό ΕΕ «82584», το οποίο έχει ενταχθεί στο Ε.Π «Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Δια Βίου Μάθηση» ΕΣΠΑ 2014 –2020 με κωδικό ΟΠΣ (MIS) «5011457» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο –ΕΚΤ) και από Εθνικούς Πόρους. Ο Ανάδοχος θα παράσχει τις σχετικές υπηρεσίες για την υποστήριξη της προσαρμογής του Πανεπιστημίου Ιωαννίνων (ΠΙ), του ΕΛΚΕ του ΠΙ, και των σχετικών συστημάτων και υποσυστημάτων τους στο Γενικό Κανονισμό για την Προστασία Δεδομένων [Κανονισμός (ΕΕ) 2016/679], σύμφωνα με την τεχνική περιγραφή που ακολουθεί.

Το προϋπολογιζόμενο κόστος ανέρχεται στο ποσό των 50.000,00€ συμπεριλαμβανομένου του αναλογούντος Φ.Π.Α.

1. **Συνοπτική περιγραφή του έργου της διακήρυξης**

Αντικείμενο του έργου αποτελεί η ανάδειξη συμβούλου για την υποστήριξη της εφαρμογής του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation) [Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27/4/2016] στο Πανεπιστήμιο Ιωαννίνων, η παροχή υπηρεσιών υποστήριξης του Υπεύθυνου/ης Προστασίας Δεδομένων (Data Protection Officer [DPO]) κατά τη διάρκεια του έργου, καθώς και η παροχή υπηρεσιών υποστήριξης της ανάπτυξης και της προσαρμογής και βελτίωσης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

Ο ανάδοχος δεσμεύεται για την παροχή υπηρεσιών υποστήριξης της υλοποίησης των απαιτήσεων του Κανονισμού (ΕΕ) 2016/679 (Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων [ΓΚΠΔ], [General Data Protection Regulation (GDPR)]) σύμφωνα με τις ανάγκες του Πανεπιστημίου Ιωαννίνων, όπως αυτές καθορίζονται παρακάτω και από την εφαρμογή του Ν. 4559/2019 (ΦΕΚ Α΄142/03.08.2018). Για την παροχή των απαιτούμενων υπηρεσιών ο ανάδοχος θα ακολουθήσει διεθνώς αναγνωρισμένες μεθοδολογίες και βέλτιστες πρακτικές, ενώ θα πρέπει να διαθέτει σχετική τεχνογνωσία και εμπειρία σε έργα σχεδίασης, ανάπτυξης αλλά και υλοποίησης Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών και Προγραμμάτων Προστασίας Δεδομένων, βασιζόμενα στα διεθνή πρότυπα, στις απαιτήσεις του νέου Γενικού Κανονισμού για την Προστασία των Δεδομένων (GDPR), καθώς επίσης και σε κοινώς αποδεκτούς κανόνες ασφάλειας σε εθνικό, Ευρωπαϊκό και διεθνές επίπεδο.

1. **Συνοπτική παρουσίαση του Πανεπιστημίου Ιωαννίνων**

To Πανεπιστήμιο Ιωαννίνων (βλ. ηλεκτρονική διεύθυνση <http://www.uoi.gr>), μετά την ψήφιση του Ν. 4559/2019 (ΦΕΚ Α΄142/03.08.2018), απαρτίζεται από 26 ακαδημαϊκά Τμήματα (βλ. ηλεκτρονική διεύθυνση <https://www.uoi.gr/ekpaideysi/sxoles-kai-tmimata/>), εκ των οποίων τα 3 θα δημιουργηθούν σε μεταγενέστερο χρόνο, κατόπιν σχετικών αποφάσεων σύμφωνα με το ισχύον θεσμικό πλαίσιο. Τα ακαδημαϊκά Τμήματα εντάσσονται σε 11 Σχολές.

Επιπροσθέτως, στο Πανεπιστήμιο Ιωαννίνων λειτουργούν επίσης Προγράμματα Μεταπτυχιακών Σπουδών υπό την εποπτεία των ακαδημαϊκών τμημάτων του ιδρύματος, καθώς επίσης και Προπτυχιακά Προγράμματα Σπουδών του πρώην ΤΕΙ Ηπείρου, τα οποία θα συνεχίσουν τη λειτουργία τους έως ότου αποφοιτήσουν οι φοιτητές/τριες που επιθυμούν να λάβουν πτυχίο ΤΕΙ και όχι πτυχίο Πανεπιστημίου.

Οι παραπάνω ακαδημαϊκές δομές έχουν τις εγκαταστάσεις τους και λειτουργούν στα Ιωάννινα, την Άρτα, την Πρέβεζα και την Ηγουμενίτσα.

Η διοικητική διάρθρωση του Πανεπιστημίου Ιωαννίνων προσδιορίζεται από:

1. Το ΠΔ 186/1999 (ΦΕΚ Α’ 173/27-8-1999) «Οργανισμός Διοικητικών Υπηρεσιών Πανεπιστημίου Ιωαννίνων».
2. Το Π.Δ. 143/2009 (ΦΕΚ 188/Α΄/29-9-2009) «Τροποποίηση του π.δ. 186/1999 Οργανισμός Διοικητικών Υπηρεσιών Πανεπιστημίου Ιωαννίνων (ΦΕΚ Α΄ 173)».
3. Την Απόφαση 9825/1-2-2018 (ΦΕΚ Β’ 448/14-2-2018) για τη σύσταση μονάδας σε επίπεδο Διεύθυνσης με τίτλο: «Διεύθυνση Οικονομικής και Διοικητικής Υποστήριξης ΕΛΚΕ».
4. Τον Ν. 4559/2018 (ΦΕΚ Α’ 142/3-8-2018) «Πανεπιστήμιο Ιωαννίνων, Ιόνιο Πανεπιστήμιο και άλλες διατάξεις».
5. Την Απόφαση 8062/7-12-2018 (ΦΕΚ Β’ 5721/19-12-2018) για τη συμπλήρωση του Οργανισμού διοικητικών υπηρεσιών του Πανεπιστημίου Ιωαννίνων στο πλαίσιο εφαρμογής των προβλέψεων του ν. 4559/2018.

Οι κεντρικές διοικητικές υπηρεσίες του ΠΙ λειτουργούν στην έδρα του Ιδρύματος, στα Ιωάννινα, ενώ παραρτήματα ή/και αυτοτελείς οργανικές μονάδες λειτουργούν στις πόλεις της Άρτας, της Πρέβεζας και της Ηγουμενίτσας.

Το προσωπικό του Πανεπιστημίου Ιωαννίνων αποτελείται από (στοιχεία 6/2021):

1. 513 μέλη ΔΕΠ,
2. 125 ΕΔΙΠ και ΕΕΠ,
3. 50 ΕΤΕΠ και
4. 309 άτομα Διοικητικό Προσωπικό.

Επίσης, στο Πανεπιστήμιο Ιωαννίνων είναι εγγεγραμμένοι (στοιχεία 6/2021):

1. 32.882 προπτυχιακοί φοιτητές/τριες,
2. 1.432 μεταπτυχιακοί φοιτητές/τριες και
3. 1.281 Υποψήφιοι Διδάκτορες.

Τέλος, στο Πανεπιστήμιο Ιωαννίνων λειτουργούν κεντρικά πληροφοριακά συστήματα που αφορούν στη διαχείριση:

1. των προπτυχιακών και μεταπτυχιακών φοιτητών (φοιτητολόγιο),
2. της υπηρεσίας διαχείρισης προσωπικού,
3. των οικονομικών και της μισθοδοσίας
4. των ερευνητικών προγραμμάτων του ΕΛΚΕ,
5. των υπηρεσιών δικτύου Δεδομένων και Φωνής,
6. των υπηρεσιών ηλεκτρονικού ταχυδρομείου,
7. της υπηρεσίας ηλεκτρονικού πρωτοκόλλου,
8. των υπηρεσιών της ΜΟΔΙΠ και της ΔΑΣΤΑ,
9. της υπηρεσίας δανεισμού βιβλίων και του ιδρυματικού αποθετηρίου, και
10. των ηλεκτρονικών μαθημάτων.
11. **Αναλυτική Περιγραφή Υπηρεσιών**

**Ο ανάδοχος θα πρέπει να συνυποβάλει στην τεχνική του προσφορά αναλυτική περιγραφή της εκτέλεσης του έργου της σύμβασης (Σχέδιο Υλοποίησης Έργου). Το** **Σχέδιο Υλοποίησης Έργου θα πρέπει να περιλαμβάνει όλα τα παρακάτω αναφερόμενα στοιχεία, συνταγμένα με τον τρόπο που περιγράφεται στην ενότητα που ακολουθεί με τίτλο «Απαιτούμενα Στοιχεία Σχεδίου Υλοποίησης».** Τεχνική Προσφορά Αναδόχου που δεν θα περιλαμβάνει Σχέδιο Υλοποίησης Έργου ή το περιλαμβανόμενο Σχέδιο Υλοποίησης Έργου δεν θα έχει συνταχθεί σύμφωνα τις παρακάτω προδιαγραφές-οδηγίες θα απορρίπτεται.

**Απαιτούμενα Στοιχεία Σχεδίου Υλοποίησης Έργου**

Τα απαιτούμενα στοιχεία του Σχεδίου Υλοποίησης Έργου είναι τα ακόλουθα:

* **Αναλυτική περιγραφή και μεθοδολογία υλοποίησης των εργασιών που θα εκτελεστούν κατά τη διάρκεια του έργου, με χρήση διακριτών ενοτήτων έργου**. Ο ανάδοχος θα επιλέξει τις ενότητες που θεωρεί κατάλληλες για την περιγραφή του έργου (π.χ. πακέτα εργασίας, φάσεις υλοποίησης, επιμέρους δράσεις, κοκ.), καθώς και τον τρόπο παρουσίασης του χρονοδιαγράμματος, των παραδοτέων ανά ενότητα εργασίας και των παραδοτέων που θεωρούνται ορόσημα (milestones) του έργου (σημειώνεται ότι η πληρωμή των παραδοτέων θα γίνεται τμηματικά για όσα παραδοτέα έχουν ολοκληρωθεί και παραληφθεί μέχρι την επίτευξη του συγκεκριμένου οροσήμου). Η περιγραφή θα πρέπει να αναφέρει τουλάχιστον τις εργασίες όπως περιγράφονται στις ενότητες του παρόντος Παραρτήματος Ι των τεχνικών προδιαγραφών (παρ. 3.1-3.7 του Παραρτήματος Ι). Κατά τη σχετική περιγραφή θα πρέπει: α) να αναφέρεται σαφώς η διάρκεια υλοποίησης των επιμέρους ενοτήτων σε μήνες -για παράδειγμα- ως εξής: Πακέτο Εργασίας 1 (Π.Ε.1): Μ1 – Μ2 (όπου Μ1 είναι ο μήνας έναρξης του Π.Ε.1 και Μ2 ο μήνας λήξης του Π.Ε.1 [συνολικά το έργο θα έχει έναρξη τον Μήνα 1 (Μ1) και λήξη τον Μήνα 8 (Μ8)]), β) να τεκμηριώνεται η διάρκεια κάθε ενότητας με αναφορά και στην αντίστοιχη ανθρωποπροσπάθεια υπό τη μορφή ανθρωπομηνών (*δεν αρκεί η απλή αναφορά μήνα έναρξης και λήξης και ανθρωπομηνών διάρκειας*), και γ) να περιγράφονται τα παραδοτέα με αναφορά του μήνα παράδοσης (Μx) και της μορφής του κάθε παραδοτέου (π.χ. έκθεση, αναφορά, υπηρεσία, μελέτη, αρχεία, λογισμικό, παραμετροποίηση λογισμικού, παραμετροποίηση συστήματος, κλπ.). Σημειώνεται ότι στα παραδοτέα θα πρέπει να περιλαμβάνονται οπωσδήποτε τα αναφερόμενα στην παρ. 4 (Παραδοτέα έγγραφα, αρχεία και μητρώα) του παρόντος Παραρτήματος. Επισημαίνεται επίσης ότι οι ανθρωπομήνες που θα χρησιμοποιηθούν στην αναλυτική περιγραφή εργασιών θα πρέπει να είναι ίδιοι με αυτούς που θα αναγραφούν στον Πίνακα Οικονομικής Προσφοράς (Παράρτημα IV).
* **Περιγραφή δομής και οργανωτικού σχήματος ομάδας έργου, προσδιορισμός αρμοδιοτήτων και ρόλων, χρονική κατανομή ανά θέμα και δραστηριότητα του έργου.** Για κάθε στέλεχος της ομάδας έργου θα πρέπει να αναφέρεται αν αποτελεί προσωπικό του αναδόχου ή εξωτερικό συνεργάτη. H ομάδα έργου του αναδόχου θα αποτελείται κατ’ ελάχιστον: α) από τον Υπεύθυνο Έργου (Project Manager) ο οποίος θα πρέπει να κατέχει πτυχίο Πανεπιστημιακής Εκπαίδευσης και να διαθέτει τουλάχιστον τριετή εμπειρία στη διοίκηση ή εκτέλεση έργων ασφάλειας πληροφοριών, β) ένα άτομο που θα προτείνεται για την υποστήριξη του Υπεύθυνου/ης Προστασίας Δεδομένων (Data Protection Officer [DPO]) του Πανεπιστημίου Ιωαννίνων, και το οποίο θα πρέπει να διαθέτει την απαραίτητη πιστοποίηση από αναγνωρισμένο φορέα για την ανάληψη και εκτέλεση των καθηκόντων DPO, όπως αυτά ορίζονται στο Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), και γ) ένα άτομο που θα προτείνεται για την υποστήριξη του Υπευθύνου Ασφάλειας Δεδομένων του Πανεπιστημίου Ιωαννίνων, ο οποίος θα πρέπει να είναι ειδικός πληροφορικής με αποδεδειγμένη γνώση και εμπειρία στην ασφάλεια δεδομένων, πληροφοριών και πληροφοριακών συστημάτων. Επίσης, επιπρόσθετα η ομάδα έργου ενδεικτικά μπορεί να περιλαμβάνει στελέχη όπως: information security consultant, IT auditor, ειδικό πληροφορικής με αποδεδειγμένη γνώση και εμπειρία στην προστασία προσωπικών δεδομένων, ειδικό πληροφορικής με αποδεδειγμένη γνώση στην ασφάλεια των πληροφοριών και των πληροφοριακών συστημάτων κλπ. Επισημαίνεται ότι η σύνθεση της ομάδας έργου παρουσιάζεται αναλυτικά από τον ανάδοχο και αποτελεί ουσιαστικό κριτήριο της βαθμολογίας της τεχνικής προσφοράς του.
* **Αναφορά και τεκμηρίωση εμπειρίας αναδόχου** **στην υλοποίηση αντίστοιχων έργων.** Βαθμολογείται η εκτέλεση των επιπλέον του ενός έργων που περιλαμβάνουν συνολικό πρόγραμμα συμμόρφωσης GDPR σε αντίστοιχους στη φύση και στο μέγεθος οργανισμούς όπως το Πανεπιστήμιο Ιωαννίνων.
* Περιγραφή της **μεθοδολογίας παρουσίασης του έργου** (στην αρχική φάση) **και της προόδου του** (σε επιλεγμένα από τον ανάδοχο χρονικά σημεία) στη Διοίκηση (Πρυτανικό Συμβούλιο και Σύγκλητος) και τους Προϊσταμένους των Διευθύνσεων του Ιδρύματος.

**Ο ανάδοχος θα πρέπει να προσφέρει κατ' ελάχιστο τις παρακάτω υπηρεσίες στο Πανεπιστήμιο Ιωαννίνων, οι οποίες θα πρέπει να περιγράφονται αναλυτικά στην τεχνική προσφορά του:**

**3.1. Επικαιροποίηση καταγραφής και αξιολόγηση της υφιστάμενης κατάστασης**

Επικαιροποίηση της αποτύπωσης της υφιστάμενης κατάστασης με τη διαδικασία συνεντεύξεων με την ανώτατη διοίκηση και τα ανώτερα στελέχη του ΠΙ. Τα υφιστάμενα μέτρα ασφαλείας και οι έλεγχοι για την προστασία των προσωπικών δεδομένων που έχουν ήδη αναπτυχθεί από την DPO, τον Υπεύθυνο Ασφάλειας Δεδομένων και τη σχετική ομάδα εργασίας του Πανεπιστημίου Ιωαννίνων, θα πρέπει να τεκμηριωθούν και να ληφθούν υπόψη.

Η πρόσβαση του αναδόχου στα δεδομένα του Πανεπιστημίου Ιωαννίνων θα γίνεται με την επίβλεψη του DPO και του Υπευθύνου Ασφαλείας Δεδομένων ή κατάλληλα εξουσιοδοτημένου προσωπικού του ιδρύματος.

***3.1.1 Δημιουργία αρχείων δεδομένων – Απεικόνιση Ροής Δεδομένων (Data Flow mapping)***

Ο ανάδοχος, σε συνεργασία και πάντοτε υπό την καθοδήγηση του DPO και του Υπευθύνου Ασφάλειας Δεδομένων του Πανεπιστημίου Ιωαννίνων, θα δημιουργήσει τα απαραίτητα αρχεία που θα πρέπει να έχει στην κατοχή του και θα μπορεί να παρουσιάζει το Ίδρυμα. Ενδεικτικά αναφέρονται:

• Κατάλογος δεδομένων προσωπικού χαρακτήρα (ποια προσωπικά δεδομένα συλλέγονται, ο σκοπός επεξεργασίας, η διαδικασία λήψης συγκατάθεσης, η πρόσβαση στα δεδομένα -εντός και εκτός του ιδρύματος-η έγγραφη και/ή η ηλεκτρονική αποθήκευσή τους, ο χρόνος διατήρησης).

• Ταξινόμηση των προσωπικών δεδομένων που έχει στην κατοχή του το ίδρυμα ανά τύπο (π.χ. ευαίσθητα, εμπιστευτικά, δημόσια).

• Προσδιορισμός διαγραμμάτων ροής για τις διάφορες ροές δεδομένων (π.χ. μεταξύ ακαδημαϊκών ή/και διοικητικών μονάδων, μεταξύ συστημάτων, μεταξύ διαδικασιών, μεταξύ χωρών).

Ο ανάδοχος θα σχεδιάσει τις φόρμες βάσει των οποίων θα γίνει η καταγραφή των αρχείων δεδομένων, καθώς επίσης και θα δημιουργήσει τα σχετικά αρχεία και τα διαγράμματα ροής δεδομένων.

***3.1.2 Έλεγχος (Audit) Πληροφοριακών Υποδομών***

Ο ανάδοχος θα πρέπει να διενεργήσει αξιολόγηση ευπάθειας (vulnerability assessment) των κεντρικών πληροφοριακών υποδομών του ΠΙ με χρήση εξειδικευμένου λογισμικού από πιστοποιημένο σε αυτή την εργασία προσωπικό του αναδόχου. Το σχετικό λογισμικό θα πρέπει να αναφέρεται στην προσφορά του αναδόχου.

**3.2 Επικαιροποίηση Προγράμματος Προστασίας Προσωπικών Δεδομένων**

Ο ανάδοχος θα αναλάβει την υποστήριξη του DPO του ΠΙ μέσω της επικαιροποίησης και της αναμόρφωσης του υφιστάμενου Προγράμματος Προστασίας Προσωπικών Δεδομένων, αποτελούμενο από Πολιτικές και Διαδικασίες για την αποτελεσματική προστασία των προσωπικών δεδομένων που διατηρεί το ΠΙ.

Ειδικότερα, ο ανάδοχος θα αναλάβει την επικαιροποίηση του υφιστάμενου Προγράμματος Προστασίας Προσωπικών Δεδομένων του ΠΙ που θα επικεντρώνεται στον τρόπο με τον οποίο θα γίνεται η συλλογή, αποθήκευση, επεξεργασία και διαχείριση των προσωπικών δεδομένων, καθώς και η συναίνεση του υποκειμένου, το δικαίωμα της διαγραφής, η καταγραφή και γνωστοποίηση παραβιάσεων (διαδικασία γνωστοποίησης της παραβίασης δεδομένων και σχέδιο απόκρισης σε περίπτωση συμβάντων), καθώς επίσης και των πολιτικών και διαδικασιών για ενημερώσεις, επιθεωρήσεις και συνεχή βελτίωση.

Ενδεικτικά το **Πρόγραμμα Προστασίας Προσωπικών Δεδομένων του ΠΙ** θα πρέπει να επικαιροποιηθεί έτσι ώστε να περιλαμβάνει τουλάχιστον τα ακόλουθα:

• Πολιτική Προστασίας Προσωπικών Δεδομένων, η οποία θα πρέπει να πληροί τις νομικές απαιτήσεις και να αντιμετωπίζει το λειτουργικό κίνδυνο και τον κίνδυνο βλάβης των υποκείμενων των δεδομένων.

• Πολιτική προστασίας προσωπικών δεδομένων των εργαζομένων, των λοιπών απασχολούμενων και των φοιτητών/φοιτητριών του Πανεπιστημίου Ιωαννίνων.

• Κώδικας Δεοντολογίας που θα περιλαμβάνει άρθρα για την Προστασία Προσωπικών Δεδομένων.

• Πολιτική και διαδικασίες για τη συλλογή και τη χρήση ευαίσθητων προσωπικών δεδομένων.

• Πολιτική και διαδικασίες για τη διατήρηση της ποιότητας των δεδομένων.

• Πολιτική και διαδικασίες για τη διαγραφή των προσωπικών δεδομένων.

• Πολιτική και διαδικασίες για δευτερεύουσες χρήσεις προσωπικών δεδομένων.

• Πολιτική και διαδικασίες για την απόκτηση έγκυρης συναίνεσης των υποκείμενων των δεδομένων.

• Πολιτική και διαδικασίες για την ασφαλή καταστροφή των προσωπικών δεδομένων.

• Πολιτική και διαδικασίες για τη χρήση των cookies και των διάφορων άλλων μηχανισμών παρακολούθησης.

• Πολιτική και διαδικασίες για τη διατήρηση των αρχείων προσωπικών δεδομένων.

• Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στη χρήση των κοινωνικών μέσων δικτύωσης από τον οργανισμό.

• Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στις πολιτικές και τις διαδικασίες της αξιοποίησης εξοπλισμού που ανήκει στους χρήστες και όχι στο ίδρυμα για την πρόσβαση στα πληροφοριακά συστήματα του ιδρύματος (Bring Your Own Device (BYOD)).

• Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων σε πρακτικές υγείας και ασφάλειας.

• Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στη χρήση καμερών (ζωντανές βιντεοδιαλέξεις, συνεδριάσεις οργάνων μέσω τηλεδιάσκεψης, κλπ).

• Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων σε πολιτικές και διαδικασίες σχετικά με την πρόσβαση στους λογαριασμούς ιδρυματικού ηλεκτρονικού ταχυδρομείου των εργαζομένων, των απασχολούμενων και των μελών της ακαδημαϊκής κοινότητας του Πανεπιστημίου Ιωαννίνων.

• Διαδικασίες ανταπόκρισης σε αιτήματα πρόσβασης σε προσωπικά δεδομένα.

• Διαδικασίες ανταπόκρισης σε αιτήματα διόρθωσης προσωπικών δεδομένων.

• 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 προσωπικών δεδομένων.

• Πολιτική και Διαδικασίες διαχείρισης των παραβιάσεων της ασφάλειας των προσωπικών δεδομένων ή της διαρροής αυτών.

• Σχέδιο αντιμετώπισης περιστατικών παραβίασης, και διατήρηση αρχείου καταγραφής παραβιάσεων (με στοιχεία όπως η φύση της παραβίασης, η εκτίμηση κινδύνου και επιπτώσεων, η προέλευση της παραβίασης, κλπ).

• Διαδικασίες κοινοποίησης των παραβιάσεων (στα ενδιαφερόμενα άτομα) και υποβολή αναφορών (σε ρυθμιστικές αρχές, πιστωτικές υπηρεσίες, κ.λπ.).

• Διαδικασίες συνεχούς παρακολούθησης και ενημέρωσης για νέες απαιτήσεις συμμόρφωσης, προτάσεις βελτίωσης και ενσωμάτωσης βέλτιστων πρακτικών.

Επίσης, θα αναλάβει την επικαιροποίηση της **Πολιτικής Προστασίας Προσωπικών Δεδομένων Συνεργατών του ΠΙ** (που αφορά τους συνεργάτες, προμηθευτές και υπεργολάβους του Πανεπιστημίου Ιωαννίνων) και θα συγγραφούν και προστεθούν κατάλληλοι όροι στα σχετικά Συμβόλαια και τις Συμβάσεις με τους Συνεργάτες. Η Πολιτική Προστασίας Προσωπικών Δεδομένων Συνεργατών θα πρέπει να περιλαμβάνει ενδεικτικά τουλάχιστον τα παρακάτω:

• Απαιτήσεις από τους συνεργάτες για την Προστασία των Προσωπικών Δεδομένων κατά την εκτέλεση συμβολαίων, συμβάσεων ή συμφωνιών.

• Όροι για δέουσα επιμέλεια σχετικά με την Προστασία των Προσωπικών Δεδομένων.

• Ειδικοί όροι για τους παρόχους υπηρεσιών αποθήκευσης νέφους (cloud).

• Άρθρα για την αντιμετώπιση περιπτώσεων μη συμμόρφωσης σε συμβόλαια, συμβάσεις και συμφωνίες ή τους όρους προστασίας προσωπικών δεδομένων που επιβάλλει ο GDPR.

Επιπλέον ο ανάδοχος θα παρέχει σχετικά κείμενα ως προς την υποχρέωση της συναίνεσης του υποκείμενου των προσωπικών δεδομένων.

**3.3 Αξιολόγηση Επιπτώσεων Προστασίας Δεδομένων – Πρόγραμμα Συμμόρφωσης – Εκτίμηση και Αντιμετώπιση/Διαχείριση Επικινδυνότητας**

***3.3.1 Αξιολόγηση Επιπτώσεων Προστασίας Δεδομένων (Data Protection Impact Assessment) και Πρόγραμμα Συμμόρφωσης (Compliance Plan)***

Ο ανάδοχος θα πρέπει να διεξάγει αξιολόγηση επιπτώσεων σχετικά με την προστασία δεδομένων (Data Protection Impact Assessment-DPIA ή Privacy Impact Assessment-PIA).

Η **αξιολόγηση επιπτώσεων προστασίας δεδομένων** θα πρέπει να περιλαμβάνει τουλάχιστον τα παρακάτω:

* Συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει το Πανεπιστήμιο Ιωαννίνων.
* 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).
* Ανάλυση των προβλεπόμενων μέτρων 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.

Κατόπιν των ανωτέρω, **ο ανάδοχος θα αναπτύξει Πρόγραμμα Συμμόρφωσης (Compliance Plan)**, το οποίο θα παρουσιάζει το σχέδιο σχετικά με τη συμμόρφωση του ΠΙ στις απαιτήσεις του GDPR και θα περιλαμβάνει τα νέα μέτρα ασφάλειας ή την αναβάθμιση των υπαρχόντων μέτρων ασφάλειας, καθώς επίσης και τον προγραμματισμό μέτρων έκτακτης ανάγκης που πρέπει να εφαρμοστούν σε περίπτωση ενδεχόμενης παραβίασης δεδομένων.

Επιπλέον, στο πλαίσιο του Προγράμματος Συμμόρφωσης θα προταθούν από τον ανάδοχο τα κατάλληλα μέτρα και οι μηχανισμοί ασφαλείας που πρέπει να υιοθετηθούν έτσι ώστε το ΠΙ να μπορεί να διαχειριστεί τον πιθανό αντίκτυπο μιας παραβίασης των προσωπικών δεδομένων.

***3.3.2 Εκτίμηση Επικινδυνότητας (Risk Assessment)***

Κατά τη φάση αυτή και λαμβάνοντας υπόψιν τους κινδύνους που εντοπίστηκαν κατά την επιθεώρηση συμμόρφωσης και την εκτίμηση αντικτύπου, ο ανάδοχος θα διεξάγει την εκτίμηση (αποτίμηση) επικινδυνότητας.

Η Εκτίμηση Επικινδυνότητας θα γίνει από τον ανάδοχο βάσει των προβλέψεων και των οδηγιών του διεθνούς και αναγνωρισμένου προτύπου ISO 27005:2018, και θα περιλαμβάνει την αποτίμηση της τρέχουσας κατάστασης και την εκτίμηση των κινδύνων για τα προσωπικά δεδομένα, των απειλών και των ευπαθειών των εξεταζόμενων πληροφοριακών συστημάτων (στα οποία είναι αποθηκευμένα τα προσωπικά δεδομένα), με την ταυτόχρονη ανάθεση υπευθυνότητας (risk owner) για κάθε ένα από τους κινδύνους. Η εκτίμηση θα γίνει με βάση την επίδραση που θα έχει η διαρροή, η αποκάλυψη ή η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή των προσωπικών δεδομένων, στα φυσικά πρόσωπα που αφορούν και στην ομαλή λειτουργία του Ιδρύματος.

***3.3.3 Αντιμετώπιση/Διαχείριση Επικινδυνότητας (Risk Treatment/Management)***

Κατά τη διαδικασία αντιμετώπισης/διαχείρισης επικινδυνότητας, η διοίκηση και ο DPO του ΠΙ με τη συμβουλευτική υποστήριξη του αναδόχου θα αποφασίσει για τη διαχείριση των κινδύνων εξετάζοντας τις λύσεις που θα προτείνει ο ανάδοχος, όπως:

* αποδοχή του επιπέδου επικινδυνότητας (risk acceptance),
* μεταβίβαση του επιπέδου επικινδυνότητας (risk transfer),
* αποφυγή του επιπέδου επικινδυνότητας (risk avoidance), και
* αντιμετώπιση του επιπέδου επικινδυνότητας (risk mitigation).

Στην αντιμετώπιση του επιπέδου επικινδυνότητας (risk mitigation), ο ανάδοχος θα προσδιορίσει και θα προτείνει τους νέους μηχανισμούς ασφάλειας που θα χρειαστεί να υιοθετηθούν, λαμβάνοντας υπόψη τους ήδη εγκατεστημένους μηχανισμούς.

**3.4 Υποστήριξη DPO του ΠΙ στον Έλεγχο Συμμόρφωσης (Compliance Audit)**

Ο ανάδοχος θα υποστηρίξει τον DPO του ΠΙ στην επιθεώρηση των σημείων αποθήκευσης των προσωπικών δεδομένων, έγγραφων και ηλεκτρονικών, την πρόσβαση σε αυτά, καθώς επίσης και τις συμφωνίες εμπιστευτικότητας που έχουν υπογραφεί, ώστε να επιβεβαιωθεί η διαφύλαξη της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των προσωπικών δεδομένων, σύμφωνα με τις απαιτήσεις του GDPR.

Επιπλέον, θα υποστηρίξει τον DPO του ΠΙ στην επιθεώρηση του τρόπου επικοινωνίας των διαφόρων με τους συνεργάτες, το είδος της πληροφορίας που ανταλλάσσεται (στην περίπτωση που ανταλλάσσονται προσωπικά δεδομένα), καθώς και τον τρόπο και τα μέσα αποθήκευσής της.

**3.5 Παρουσίαση των ευρημάτων των επιθεωρήσεων συμμόρφωσης, της Αξιολόγησης Επιπτώσεων Προστασίας Δεδομένων, καθώς και της Εκτίμησης και Αντιμετώπισης/Διαχείριση Επικινδυνότητας στον DPO και τη Διοίκηση του ΠΙ**

Ο ανάδοχος θα παρουσιάσει στον DPO και τη Διοίκηση του ΠΙ τα αποτελέσματα των επιθεωρήσεων συμμόρφωσης, καθώς επίσης και τα αποτελέσματα της αξιολόγησης των επιπτώσεων της Προστασίας Δεδομένων, καθώς επίσης και την εκτίμηση και την αντιμετώπιση και διαχείριση της επικινδυνότητας.

Επίσης, θα αναλυθούν οι μεγαλύτεροι κίνδυνοι που αντιμετωπίζει το ΠΙ όσον αφορά τα προσωπικά δεδομένα, τους διαχειριστές προσωπικών δεδομένων, καθώς επίσης και τα προτεινόμενα μέτρα και ενέργειες αποκατάστασης προκειμένου να μετριαστούν επαρκώς οι κίνδυνοι που εντοπίστηκαν.

Τέλος, στο πλαίσιο αυτό, ο ανάδοχος θα τηρεί Αρχείο Δραστηριοτήτων.

**3.6 Υπηρεσίες Υποστήριξης Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer [DPO]).**

O ανάδοχος θα παρέχει στο ΠΙ, κατάλληλα καταρτισμένο και πιστοποιημένο άτομο, προκειμένου να υποστηρίξει τον Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer [DPO]) που έχει οριστεί ήδη από το Πανεπιστήμιο Ιωαννίνων, σύμφωνα με τα οριζόμενα στο άρθρο 39, παρ. 1 του Γενικού Κανονισμού για την Προστασία των Δεδομένων (General Data Protection Regulation - GDPR). Η διάρκεια παροχής των υπηρεσιών υποστήριξης του DPO του Πανεπιστημίου Ιωαννίνων θα είναι ίση με τη διάρκεια της σύμβασης (8 μήνες από την υπογραφή της ή το αργότερο έως τη λήξη του φυσικού αντικειμένου του Υποέργου 3), και οι σχετικές υπηρεσίες θα παρέχονται από την ημερομηνία υπογραφής της μέχρι και την ημερομηνία λήξης αυτής. Ο/Η υπεύθυνος/η υποστήριξης του DPO του Πανεπιστημίου Ιωαννίνων θα πλαισιώνεται από κατάλληλη υποστηρικτική ομάδα του αναδόχου, η τεχνογνωσία και κατάρτιση της οποίας θα καλύπτει όλες τις απαιτήσεις συμμόρφωσης προς το Γενικό Κανονισμό για την Προστασία των Δεδομένων (General Data Protection Regulation - GDPR). Η σύνθεση της υποστηρικτικής ομάδας θα είναι επιλογή του αναδόχου και θα περιγράφεται αναλυτικά στην τεχνική του προσφορά.

Ο/Η υπεύθυνος/η υποστήριξης του DPO θα συνδράμει τον DPO του Πανεπιστημίου Ιωαννίνων στην παρακολούθηση, αναθεώρηση και βελτίωση του Προγράμματος Προστασίας Προσωπικών Δεδομένων που θα αναπτύξει και θα εφαρμόσει το ΠΙ, με βάση τις απαιτήσεις του νέου Κανονισμού για την προστασία των προσωπικών δεδομένων. Επιπλέον, θα υποστηρίζει τον DPO του Πανεπιστημίου Ιωαννίνων στην παρακολούθηση της εφαρμογής των τεχνικών και οργανωτικών μέτρων που έχει δεσμευτεί να πραγματοποιήσει το ΠΙ στο Πρόγραμμα Συμμόρφωσης (Compliance Plan), θα επικαιροποιεί τις εκθέσεις Αξιολόγησης Επιπτώσεων Προστασίας Δεδομένων (Data Protection Impact Assessments,DPIAs) που έχουν δημιουργηθεί για τις επεξεργασίες προσωπικών δεδομένων υψηλού ρίσκου, θα δημιουργεί νέες DPIAs για νέες επεξεργασίες προσωπικών δεδομένων υψηλού ρίσκου, θα υποστηρίζει τις ενημερώσεις του προσωπικού και τις εσωτερικές επιθεωρήσεις, με στόχο την επίτευξη του βέλτιστου επιπέδου προστασίας των προσωπικών δεδομένων.

Στο πλαίσιο των σχετικών υπηρεσιών, ο ανάδοχος θα παρέχει συμβουλευτικές υπηρεσίες στον Υπεύθυνο Προστασίας Δεδομένων (DPO) και την ομάδα που θα τον/την πλαισιώνει από το προσωπικό του Πανεπιστημίου για την περίοδο μέχρι τη λήξη της παρούσας σύμβασης. Οι παραπάνω συμβουλευτικές υπηρεσίες θα τεκμηριώνονται με Εκθέσεις Υποστήριξης (report) η οποία θα παραδοθεί τρεις μήνες πριν την λήξη της παρούσας σύμβασης.

1. **Παραδοτέα έγγραφα, αρχεία και μητρώα**

Στο πλαίσιο του έργου, θα παραδοθούν στο Πανεπιστήμιο Ιωαννίνων κατ' ελάχιστο τα παρακάτω έγγραφα, αρχεία και μητρώα:

* Personal Data Register: Η αναφορά αυτή θα περιλαμβάνει κατηγοριοποιημένα τα προσωπικά δεδομένα του Πανεπιστημίου Ιωαννίνων, όπως αυτά προσδιορίστηκαν και ταξινομήθηκαν.
* Data Flow Mapping: Αρχεία και μητρώα επεξεργασίας, διαγράμματα ροής των προσωπικών δεδομένων (απεικόνιση των προσωπικών δεδομένων, της επεξεργασίας, της πρόσβασης σε αυτά κ.λπ.).
* Πρόγραμμα συμμόρφωσης (Compliance Plan): Το έγγραφο θα παρουσιάζει το σχέδιο σχετικά με τη συμμόρφωση του ΠΙ με τις απαιτήσεις του GDPR και θα περιλαμβάνει τα νέα μέτρα ασφάλειας ή την αναβάθμιση των υπαρχόντων μέτρων ασφάλειας, καθώς επίσης και τον προγραμματισμό μέτρων έκτακτης ανάγκης που πρέπει να εφαρμοστούν σε περίπτωση παραβίασης δεδομένων.
* Risk Assessment & Risk Treatment: Η αναφορά αυτή, θα παρουσιάζει τις τιμές των απειλών και των ευπαθειών για κάθε μία από τις κατηγορίες των προσωπικών δεδομένων του personal data register, τους μηχανισμούς ασφάλειας που πρέπει να εγκατασταθούν ώστε να αντιμετωπιστούν οι κίνδυνοι που διαφάνηκαν κατά την αποτίμηση επικινδυνότητας, καθώς επίσης και τους risk owners.
* Data Protection Impact Assessment(s): Η αναφορά αυτή, θα παρουσιάζει τις επιπτώσεις των σχεδιαζόμενων πράξεων επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.
* Compliance Audit Report: Η έκθεση αυτή θα παρουσιάσει τα ευρήματα των επιθεωρήσεων συμμόρφωσης, η οποία θα παρέχει πληροφορίες σχετικά με τα κενά συμμόρφωσης που εντοπίστηκαν κατά τους ελέγχους συμμόρφωσης της εταιρίας και προτάσεις βελτίωσης.
* Personal Data Protection Policies and Procedures: Οι Πολιτικές, Διαδικασίες και Οδηγίες Προστασίας Προσωπικών Δεδομένων, όπως αυτές έχουν περιγραφεί αναλυτικά στην ενότητα «3.2 Επικαιροποίηση Προγράμματος Προστασίας Προσωπικών Δεδομένων».

**ΜΕΡΟΣ Β- ΟΙΚΟΝΟΜΙΚΟ ΑΝΤΙΚΕΙΜΕΝΟ ΤΗΣ ΣΥΜΒΑΣΗΣ**

Η σύμβαση περιλαμβάνεται στο έργο με τίτλο «ΠΡΟΣΑΡΜΟΓΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ / ΥΠΟΣΥΣΤΗΜΑΤΩΝ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΙΩΑΝΝΙΝΩΝ ΚΑΙ ΤΟΥ ΕΛΚΕ, ΣΤΟ ΝΕΟ ΚΑΝΟΝΙΣΜΟ ΓΙΑ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ» (Υποέργο 3), της Πράξης «Δράσεις υποστήριξης της λειτουργίας του Ειδικού Λογαριασμού Κονδυλίων Έρευνας του Πανεπιστημίου Ιωαννίνων, ως δικαιούχου στη διαχείριση και υλοποίηση παρεμβάσεων του ΕΠΑΝΑΔΕΔΒΜ» με κωδικό Επιτροπής Ερευνών «82584» και κωδικό MIS «5011457».

Η Πράξη συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο –ΕΚΤ) και από Εθνικούς Πόρους, στο πλαίσιο του Επιχειρησιακού Προγράμματος Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Δια Βίου Μάθηση» ΕΣΠΑ 2014 –2020 (αριθ. ενάριθ. 2018ΣE34510224).

Η εν λόγω Προμήθεια εντάσσεται στον ακόλουθο κωδικό του Κοινού Λεξιλογίου δημοσίων συμβάσεων (CPV): 72322000-8

Η εκτιμώμενη καθαρή αξία της σύμβασης ανέρχεται στο ποσό των **40.322,58€** ήτοι συνολικής αξίας **50.000,00€** συμπεριλαμβανομένου ΦΠΑ.

**Η διάρκεια της σύμβασης ορίζεται σε οκτώ (8) μήνες, από την ημερομηνία υπογραφής της σύμβασης, ή το αργότερο μέχρι τη λήξη του φυσικού αντικειμένου του έργου.**

O Συντάξας των Τεχνικών Προδιαγραφών

Καθηγήτης Τριαντάφυλλος Αλμπάνης

Πρύτανης Πανεπιστημίου Ιωαννίνων