Piraeus, 01/12/2025

SUBJECT: **Clarifications (part 1) regarding the tender for the "Provision of Combined Gap Analysis Services in accordance with ISO 27001:2022 and the NIS2 Directive (Law 5160/2024)"**

Interested parties are kindly requested to refer to all additional information and/or clarifications provided by PPA S.A., regarding the questions received so far in relation to the in subject tender.

The said replies constitute an integral part of the Invitation.

QUESTION 1:

"… θα θέλαμε να επισημάνουμε τα κάτωθι:

1. Μελετώντας προσεκτικά τα απαιτούμενα Παραδοτέα (7.1), παρατηρούμε ότι στα σημεία Α.2 («Implementation schedule and cost estimation for each proposed compliance action and deviation correction») και Β.3 («Comprehensive Compliance Plan with prioritized proposals for corrective technical and organizational measures, accompanied by a timeline and cost estimation per measure»), ζητείται η παροχή εκτίμησης κόστους (cost estimation) για την εφαρμογή των προτεινόμενων διορθωτικών τεχνικών και οργανωτικών μέτρων.

Επιθυμούμε να εκφράσουμε μία σημαντική επιφύλαξη σχετικά με αυτή την απαίτηση:

Η κοστολόγηση μέτρων που προτείνονται από τον ίδιο τον Ανάδοχο του Gap Analysis δημιουργεί σοβαρό ζήτημα σύγκρουσης συμφερόντων. Αυτό υπονομεύει την αντικειμενική και ανεξάρτητη φύση της συμβουλευτικής υπηρεσίας, καθώς ο Ανάδοχος θα μπορούσε ενδεχομένως να διεκδικήσει την υλοποίηση των έργων στο μέλλον.

Η ακριβής κοστολόγηση της εφαρμογής (η οποία διαφέρει από μια εκτίμηση μεγέθους) καθίσταται ιδιαίτερα δυσχερής και επισφαλής από έναν Σύμβουλο Gap Analysis. Αυτό συμβαίνει διότι δεν έχει πρόσβαση στις τελικές εμπορικές προσφορές, στις τιμές αδειών χρήσης, ή στις ειδικές απαιτήσεις υλοποίησης που θα καθοριστούν από τον μελλοντικό Ανάδοχο Υλοποίησης/Προμήθειας.

Λαμβάνοντας υπόψη τα ανωτέρω, θεωρούμε σκόπιμο να αφαιρεθεί η εν λόγω υποχρέωση από το scope της συγκεκριμένης πρόσκλησης. Εναλλακτικά παρακαλούμε όπως μας επισημάνετε με ποιον τρόπο επιθυμείτε να γίνει η εκτίμηση του κόστους προκειμένου να διασφαλιστεί η αμερόληπτη παροχή της συμβουλευτικής υπηρεσίας (Gap Analysis) και η απουσία σύγκρουσης συμφερόντων.

Όπως προβλέπεται στα Παραδοτέα 7.1 (Α.2) και 7.1 (Β.3) της Πρόσκλησης, η παροχή ενδεικτικής εκτίμησης κόστους ανά προτεινόμενο διορθωτικό μέτρο αποτελεί αναπόσπαστο μέρος του έργου.

Η εν λόγω εκτίμηση δεν αποτελεί εμπορική προσφορά, δεν δημιουργεί δεσμευτικό κόστος ούτε προδικάζει με οποιονδήποτε τρόπο μελλοντικές διαδικασίες προμήθειας ή υλοποίησης.

Η εκτίμηση θα βασίζεται αποκλειστικά στην επαγγελματική τεχνογνωσία του Συμβούλου και σε διαθέσιμα στοιχεία αγοράς, χωρίς να επηρεάζει ή να συνδέεται με οποιαδήποτε μελλοντική διαδικασία υλοποίησης.

Συνεπώς, η απαίτηση παραμένει ως έχει στην Πρόσκληση.

As stated in Articles 7.1(A.2) and 7.1(B.3) of the Tender, the provision of an indicative cost estimation per corrective measure is an integral part of the required deliverables.

The estimation does not constitute a commercial offer, binding price, or procurement commitment.

It solely reflects the consultant's professional assessment based on best practice and available market benchmarks and does not prejudge any future procurement or implementation process.

The requirement therefore remains as specified in the Tender.

2. *Στο 2. SCOPE OF TENDER αναφέρεται «The services will include: (a) conducting a comprehensive Gap Analysis according to ISO 27001:2022; (b) conducting a Gap Analysis in line with the NIS2 Directive and the relevant national cybersecurity framework decisions; and (c) preparing a Consolidated Gap Analysis Report identifying the current compliance status, deviations, and a proposed action plan to achieve full alignment with both frameworks. The outcomes of the project will support PPA in the development and certification of an integrated Information Security Management System (ISMS) within its existing Integrated Management System (IMS) and enhance compliance level with NIS 2 requirements» παρακαλώ διευκρινίστε αν το Gap Analysis περιλαμβάνει μόνο τεχνικά μέτρα, ή θα περιλαμβάνει και συστημικά θέματα.*

Το Gap Analysis περιλαμβάνει τόσο τεχνικά όσο και οργανωτικά/συστημικά μέτρα

The Gap Analysis covers both technical and organizational/systemic measures

3. *Σύμφωνα με τα απαιτούμενα στο 2. SCOPE OF TENDER «The outcomes of the project will support PPA in the development and certification of an integrated Information Security Management System (ISMS) within its existing Integrated Management System (IMS) and enhance compliance level with NIS 2 requirements» στο πλαίσιο εκτέλεσης του έργου δεν περιλαμβάνεται η Ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας πληροφοριών σύμφωνα με το πρότυπο ISO 27001:2022 όπως επίσης ούτε η ανάπτυξη τεκμηρίωσης για τις απαιτήσεις του NIS 2, (ενδεικτικώς: εγχειρίδιο, πολιτικές, διαδικασίες, αρχεία, έντυπα) παρακαλώ επιβεβαιώστε ή διευκρινίστε διαφορετικά.*

Στο έργο δεν περιλαμβάνεται η Ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας πληροφοριών σύμφωνα με το πρότυπο ISO 27001:2022, ούτε η ανάπτυξη τεκμηρίωσης για τις απαιτήσεις του NIS 2, π.χ. εγχειρίδιο, πολιτικές, διαδικασίες, αρχεία, έντυπα.

The project does not include the development of an Information Security Management System (ISMS) in accordance with ISO 27001:2022, nor the development of any documentation required under NIS2, such as manuals, policies, procedures, records, or forms.

4. Το Gap Analysis Report για τη συμμόρφωση με το νόμο 5160/2024 (NIS2) γίνεται σύμφωνα με το εργαλείο συμμόρφωσης της Εθνικής Αρχής Κυβερνοασφάλειας (Deliverables B.2.), που περιλαμβάνει και τις απαιτήσεις του ανωτέρω νόμου (Deliverables B.1.) και δεν πρόκειται για δύο διαφορετικά Gap Analysis Report. Το παραδοτέο B.1. και B.2. αντιστοιχούν στο ίδιο έγγραφο, παρακαλώ επιβεβαιώστε.

Τα Παραδοτέα B.1 και B.2 είναι διακριτά:

B.1: Gap Analysis Report βάσει των απαιτήσεων του N. 5160/2024 (NIS2).

B.2: Αποτύπωση του Gap Analysis σύμφωνα με το Εργαλείο Αυτοαξιολόγησης Συμμόρφωσης της Εθνικής Αρχής Κυβερνοασφάλειας.

Παρότι σχετίζονται με το ίδιο κανονιστικό πλαίσιο, αποτελούν ξεχωριστά παραδοτέα όπως ορίζεται στην Πρόσκληση.

Deliverables B.1 and B.2 concern distinct reporting requirements.

B.1 refers to the Gap Analysis Report against the requirements of Law 5160/2024 (NIS2).

B.2 concerns the structured assessment output aligned with the Entity Compliance Assessment Tool of the National Cybersecurity Authority.

While both relate to the same regulatory framework, they constitute separate deliverables as explicitly defined.

5. Παρακαλώ όπως αποστείλετε το ANNEX A & B σε μορφή word.