AVVISO PER LA MANIFESTAZIONE DI INTERESSE PER L'AFFIDAMENTO DI UN SERVIZIO DI ANALISI DEL SITO WEB PER CONFORMITA' GDPR, AVA3 E PENETRATION TEST

Finalità

L'Università degli Studi di Palermo è in fase di accreditamento secondo il nuovo modello di AVA3 predisposto da ANVUR. L'attività riguarderà in modo significativo il portale di Ateneo che sarà utilizzato dai CEV per reperire la documentazione.

I controlli AVA3 sottolineano l'importanza di presentare i contenuti in maniera trasparente e facilmente reperibili, anche attraverso il sito internet, per docenti, studenti e tutte le parti interessate, garantendo che l'università diffonda efficacemente le proprie politiche e i risultati ottenuti in ambito qualitativo. Inoltre, al fine di verificare i requisiti di sicurezza del sito web di Ateneo si intende predisporre un'analisi approfondita di tutte le sezioni web per evidenziare eventuali vulnerabilità.

Oggetto della fornitura

Ciò premesso l'Amministrazione intende avvalersi di servizi professionali finalizzati all'espletamento delle seguenti attività:

- Conformità al GDPR
  - Minimizzazione del rischio di incorrere in sanzioni e penalità derivanti da non conformità.
  - Tutela dei dati personali e miglioramento della percezione di sicurezza e affidabilità da parte degli studenti e del personale, con conseguente rafforzamento della fiducia nel brand dell'Università.
- Sicurezza in ambito di Cybersecurity
  - Salvaguardia dei dati sensibili e della proprietà intellettuale

dell'ateneo contro accessi non autorizzati e cyber attacchi.

- Assicurazione di un funzionamento costante delle attività didattiche e amministrative, anche in caso di tentativi di intrusione.

- Trasparenza
  - Dimostrazione di responsabilità e integrità nelle operazioni, rafforzando la legittimità agli occhi di tutti gli stakeholder.
  - Facilitazione nel processo decisionale degli studenti e delle loro famiglie grazie alla disponibilità di informazioni complete e tempestive.
  - Miglioramento della qualità del processo valutativo da parte di ANVUR

Nello specifico, relativamente alle diverse attività individuate:

GDPR

- Ricerca e analisi dei cookie e dei sistemi di tracciamento: scansione del sito internet attraverso l'utilizzo del tool "WebsiteAudit" dell'European Data Protection Board;
- Analisi del sito web: verifica puntuale e rilevazione delle non conformità alla luce delle linee guida del EDPB del Maggio 2020;
- Report: Produzione di un report di conformità che evidenzi le non conformità
- Produzione documentale: erogare tutta la documentazione eventualmente necessaria per garantire la compliance normativa del sito web.

- Scansione del sito web attraverso «WebsiteAudit» dell'EDPB
- Analisi e classificazione dei cookie individuati
- Ricerca di ulteriori metodi di tracciamento
- Analisi puntuale di ogni pagina del sito e studio delle interazioni «sito web/utente»
- Verifica formale delle conformità/non conformità

alla luce della normativa vigente in ambito privacy:

✓ Regolamento (UE) 679/2016

✓ Provvedimento del Garante 231/2020

✓ Guidelines (EDPB) 05/2020 on consent under Regulation (UE) 2016/679

✓ D.Lgs 196/2003 modificato dal D.Lgs del 10 agosto 2018, n. 101, e le novelle introdotte dal decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205 e dal decreto-legge 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178

- Rilascio di un Report contenente:

✓ i driver e i sotto-driver di analisi rispetto alla normativa in esame;

✓ gli elementi ritenuti non conformi

✓ gli elementi ritenuti migliorabili nel rispetto del principio di accountability (responsabilità del titolare)

✓ il piano di rientro puntuale per ogni driver utilizzato

✓ il suggerimento e la ricerca di eventuali soluzioni software di mercato (se applicabile)

- Produzione e/o adeguamento di:

✓ privacy policy

✓ cookie policy

✓ testi per il cookie banner

WAP

1. Information Gathering

Identificazione delle informazioni sull'applicazione web, comprese le tecnologie utilizzate (linguaggi di programmazione, framework, CMS), la

tipologia dell'architettura (front-end, back-end, database), e i possibili vettori di attacco

2. Vulnerability Analysis

Identificazione e analisi delle vulnerabilità. In questa fase vengono utilizzati sia strumenti automatici che un approccio manuale.

3. Exploitation

Le potenziali vulnerabilità vengono analizzate, classificate e sfruttate.

4. Reporting

Creazione della reportistica, sia Executive che Technical, comprese azioni di rimedio suggerite.

AVA3

- Analisi: Studio delle linee guida Anvur (https://www.anvur.it/attivita/ava/accreditamento-periodico/modello-ava3/strumenti- di-supporto/) e identificazione dei controlli relativi al sito web;
- Normalizzazione dei controlli: Interpretazione delle linee guida AVA3 e costruzione degli appositi controlli idonei a tradurre i requisiti previsti da ANVUR;
- Rilevazione dei Gap: Rilascio di un report comprendente il piano di rientro utile a colmare le non conformità rilevate.

Requisiti di partecipazione

Le suddette attività dovranno essere integralmente completate entro 45 giorni dall'affidamento dell'incaricato.

Potranno presentare proprie offerte operatori economici, in possesso dei requisiti di partecipazione e delle competenze in materia cybersecurity, GDPR, modello AVA3.

Possono presentare la domanda di partecipazione i soggetti che alla data di presentazione della domanda siano in possesso dei seguenti requisiti:

1. competenze professionali nelle tematiche oggetto della manifestazione di interesse;
2. pieno godimento dei diritti civili e politici;
3. non aver riportato condanne penali per reati che comportano una pena detentiva o l'interdizione, anche temporanea, dai pubblici uffici;
4. possesso dei requisiti di indipendenza e obiettività di cui all'art. 10 del D. Lgs. n. 39/2010;
5. aver maturato, negli ultimi tre anni decorrenti dalla pubblicazione del presente avviso, un'esperienza professionale triennale presso soggetti pubblici e/o privati soggetti a controllo pubblico, nell'attività oggetto della manifestazione di interesse;
6. assenza di cause di incompatibilità ed ineleggibilità previste dalla normativa;
7. requisiti di ordine generale di cui agli artt. 94 e 95 del D. Lgs. 36/2023;
8. iscrizione alla piattaforma di e-procurement MEPA.

L'offerta economica relativa alle prestazioni richieste deve essere espressa al ribasso dell'importo massimo di € 26.000,00 (euro ventiseimila/00) al netto di IVA.

Modalità di selezione delle offerte

La selezione delle offerte avverrà sulla scorta dell'offerta tecnica presentata e sulla base del prezzo offerto, mediante l'attribuzione un punteggio massimo pari a 10 punti secondo il seguente schema:

Offerta Tecnica: massimo 8 punti, secondo i seguenti criteri.

- qualità tecnica della proposta (intendendo per tale la pertinenza e corrispondenza degli obiettivi indicati, la congruenza con i requisiti tecnici e operativi richiesti, le caratteristiche funzionali e

metodologiche, la pianificazione delle attività e l'organizzazione del progetto riguardo a obiettivi e tempi) (max 4 punti)

- esperienza pregressa nella fornitura, in particolare a enti pubblici, di servizi analoghi a quelli oggetto di affidamento e competenza del personale utilizzato nell'esecuzione dell'appalto (max 4 punti)

Offerta economica massimo 2 punti secondo la formula (Punti offerta= (Valore miglior ribasso/ Valore ribasso offerto) X 2.

Termini e modalità di presentazione delle offerte

A pena di esclusione, i soggetti interessati dovranno presentare, entro 7 giorni dalla pubblicazione del presente invito sull'albo di Ateneo, propria istanza firmata con firma digitale, tramite PEC a pec@cert.unipa.it, contenente i riferimenti generali secondo il modello allegato, la relazione tecnica, un'offerta economica. Non verranno prese in considerazione offerte che eccedano l'importo previsto dalla manifestazione di interesse o che siano inviate successivamente alla scadenza indicata.

L'Università si riserva di procedere a verifiche in ordine alla veridicità dei dati dichiarati, anche dopo la definizione della procedura di affidamento dell'incarico, procedendo alla revoca dello stesso affidamento in caso di dichiarazione mendaci. A seguito di individuazione dell'operatore economico sarà avviata trattativa diretta su piattaforma acquinstiretepa.it.

Codice in materia di protezione dei dati personali

Ai sensi e per gli effetti di dall'art. 13 del GDPR regolamento UE (Regolamento Generale sulla protezione dei dati UE679/16) con la partecipazione alla presente procedura l'Operatore economico presta il proprio assenso al trattamento dei propri dati personali. L'assenso al trattamento dati per le finalità sopra indicate è obbligatorio.

Titolare del trattamento ai sensi del Regolamento UE 679/2016 (di seguito GDPR"), è l'Università degli Studi di Palermo, con sede legale in Piazza Marina, 61. L'Università degli Studi di Palermo informa che i dati personali forniti ovvero altrimenti acquisiti nel corso del rapporto, formeranno oggetto di operazioni di trattamento nel rispetto della normativa sopracitata e dagli obblighi di riservatezza. In particolare:

I dati personali forniti verranno trattati per consentire una efficace gestione dei rapporti commerciali e l'adempimento delle obbligazioni contrattuali; consentire l'esercizio dei diritti e interessi legittimi del Titolare; consentire l'adempimento delle obbligazioni previste dalle normative vigenti.

I dati saranno trattati sia con strumenti/supporti cartacei che elettronici/informatici/telematici, nel pieno rispetto delle norme di legge, secondo principi di liceità e correttezza ed in modo da tutelare la riservatezza Nell'ambito delle finalità su menzionate, i dati possono essere comunicati ai dipendenti e collaboratori all'interno della struttura del Titolare nella loro qualità di incaricati del trattamento, i quali li tratteranno secondo le disposizioni specificatamente impartire.

All'esterno della struttura del Titolare, i dati possono essere comunicati ai collaboratori esterni che si occupano di fornire servizi al Titolare in qualità di Responsabili del trattamento o Titolari autonomi.

I dati, inoltre, possono essere comunicati a tutti quei soggetti pubblici e privati la cui facoltà di accedere ai dati sia riconosciuta da disposizioni di legge o da ordini delle autorità.

Nessuno dei dati personali sarà oggetto di diffusione, salvi i casi di legge.

ALLEGATO 1
MITTENTE
_____
_____
_____

All'Università degli Studi di Palermo
Piazza Marina, 61
90133 - Palermo
PEC: pec@cert.unipa.it

"Presentazione offerta per assessment sito web di Ateneo "

Il sottoscritto _____

Nato a _____, il _____

nella sua qualità di _____

della _____

con sede legale in _____,
via/piazza_____ n. _____
e sede operativa in _____,
via/piazza_____ n. _____
Partita IVA _____ e Codice Fiscale _____
telefono _____ Fax _____
PEC _____ e-mail _____

PRESENTA

la propria offerta relativamente alle attività indicate nella manifestazione di interesse.
La fornitura prevede i seguenti servizi professionali:

- Conformità al GDPR
  - Minimizzazione del rischio di incorrere in sanzioni e penalità derivanti da non conformità.
  - Tutela dei dati personali e miglioramento della percezione di sicurezza e affidabilità da parte degli studenti e del personale, con conseguente rafforzamento della fiducia nel brand dell'Università.

- Sicurezza in ambito di Cybersecurity
  - Salvaguardia dei dati sensibili e della proprietà intellettuale dell'ateneo contro accessi non autorizzati e cyber attacchi.
  - Assicurazione di un funzionamento costante delle attività didattiche e amministrative, anche in caso di tentativi di intrusione.
- Trasparenza
  - Dimostrazione di responsabilità e integrità nelle operazioni, rafforzando la legittimità agli occhi di tutti gli stakeholder.
  - Facilitazione nel processo decisionale degli studenti e delle loro famiglie grazie alla disponibilità di informazioni complete e tempestive.
  - Miglioramento della qualità del processo valutativo da parte di ANVUR

Sin da ora il sottoscritto si impegna a svolgere il servizio in perfetta regolarità assumendosene il relativo rischio e fornendo personale qualificato ed esperto.
Ai sensi degli articoli 46 e 47 del D.P.R. 28/12/2000 n. 445, consapevole delle sanzioni penali previste dall'articolo 76 del medesimo D.P.R. 445/2000 per le ipotesi di falsità in atti e dichiarazioni mendaci

DICHIARA

1.di possedere le competenze professionali nelle tematiche oggetto della manifestazione di interesse;

2. di godere a pieno dei diritti civili e politici;
3. di non aver riportato condanne penali per reati che comportano una pena detentiva o l'interdizione, anche temporanea, dai pubblici uffici;
4. di essere in possesso dei requisiti di indipendenza e obbiettività di cui all'art. 10 del D. Lgs. n. 39/2010;
5. di aver maturato, negli ultimi tre anni decorrenti dalla pubblicazione del presente avviso, un'esperienza professionale triennale presso soggetti pubblici e/o privati soggetti a controllo pubblico, nell'attività prevista dal presente avviso;
6. di non trovarsi in cause di incompatibilità ed ineleggibilità previste dalla normativa;
7. di essere in possesso dei requisiti di ordine generale di cui agli artt. 94 e 95 del D. Lgs. 36/2023;
8. di essere iscritto alla piattaforma di e-procurement MEPA;

9. di aver preso piena visione, accettandolo, dell'avviso di Selezione per la fornitura di un SERVIZIO DI ANALISI DEL SITO WEB PER CONFORMITA' GDPR, AVA3 E PENETRATION TEST.

Si allegano:

a) documentazione che evidenzia l'esperienza professionale triennale presso soggetti pubblici e/o privati soggetti a controllo pubblico, nell'attività oggetto della manifestazione di interesse
b) relazione tecnica dettagliata circa le modalità operative dell'attività;
c) fotocopia di un documento d'identità in corso di validità del soggetto che sottoscrive la dichiarazione/candidatura o del legale rappresentante in caso di società;
d) offerta economica

Con la sottoscrizione della presente fornisco assenso al trattamento dei dati personali, finalizzato alla gestione della procedura di selezione e degli adempimenti conseguenti ai sensi **dall'art. 13 del GDPR regolamento UE (Regolamento Generale sulla protezione dei dati UE 679/16)**

_____, il _____ Timbro e/o Firma
_____