CITTÀ METROPOLITANA DI PALERMO

DIREZIONE GARE CONTRATTI INNOVAZIONE TECNOLOGICA

ALLA C.A. ……

Giusta Determinazione Dirigenziale n. … del … la S.V. è stata nominata componente della Commissione giudicatrice per la Concorso di Progettazione a procedura aperta, ai sensi dell’art.60 del D.Lgs. 50/2016 e ss.mm.ii., in due gradi, in modalità informatica, riguardante **“Cittadella dello studente c.da Santa Marina in Bagheria. Realizzazione di un nuovo istituto scolastico con annessa area mensa, area destinata a verde sport e spettacolo a servizio degli Istituti scolastici di Bagheria”** che si svolge in pieno anonimato attraverso l’apposita piattaforma telematica che è stata messa a disposizione gratuitamente dal Consiglio Nazionale Architetti Pianificatori Paesaggisti e Conservatori, giusta Protocollo d’Intesa prot. n° 9548 del 7/02/2023 tra la Città Metropolitana di Palermo e il Consiglio Nazionale degli Architetti Pianificatori Paesaggisti e Conservatori.
Conformemente a quanto stabilito dal Regolamento UE 679/2016, dalla normativa italiana vigente D.Lgs. 196/2003 e ss.mm.ii. e dall'art. 5 comma 1 del "Regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali" approvato con Decreto del Sindaco Metropolitano n. 137 del 23/12/2019, si incarica la S.V. quale Incaricato del trattamento dei dati personali gestiti al fine di adempiere alle attività operative assegnate dal Titolare nell’ambito del rapporto lavorativo intercorrente tra la sua persona e lo stesso Titolare del trattamento dei dati. In particolare, in relazione alle seguenti banche dati:
- DOCUMENTAZIONE DELLA GARA “Concorso di Progettazione a procedura aperta, ai sensi dell’art.60 del D.Lgs. 50/2016 e ss.mm.ii., in due gradi, in modalità informatica, riguardante - Cittadella dello studente c.da Santa Marina in Bagheria. Realizzazione di un nuovo istituto scolastico con annessa area mensa, area destinata a verde sport e spettacolo a servizio degli Istituti scolastici di Bagheria - CIG: 9647303648”
- PROCEDURA TELEMATICA RELATIVA ALLA GARA “Concorso di Progettazione a procedura aperta, ai sensi dell’art.60 del D.Lgs. 50/2016 e ss.mm.ii., in due gradi, in modalità informatica, riguardante - Cittadella dello studente c.da Santa Marina in Bagheria. Realizzazione di un nuovo istituto scolastico con annessa area mensa, area destinata a verde sport e spettacolo a servizio degli Istituti scolastici di Bagheria - CIG: 9647303648”

Nell’ambito dell’espletamento delle proprie funzioni, si raccomanda l’adozione ed il monitoraggio delle seguenti misure di sicurezza, atte a impedire eventuali accessi abusivi ai dati personali detenuti sotto la responsabilità del Titolare del trattamento.

In ottemperanza al RGPD, che disciplina la protezione delle persone fisiche con riferimento al trattamento dei dati personali, le SS.LL. sono autorizzate a trattare i dati personali, nonché le eventuali categorie particolari di dati di cui agli artt. 9 e 10 del RGPD, strettamente necessari per l’istruttoria e la definizione dei procedimenti amministrativi di competenza della Commissione giudicatrice nominata con la Determinazione Dirigenziale n. ... del ..., secondo le indicazioni di seguito dettagliate.

Il componente della Commissisone giudicatrice, individuato quale Incaricato al trattamento dei dati é legittimato:

- a trattare i dati personali di cui vengano a conoscenza nell’ambito dello svolgimento della propria attività istituzionale in modo lecito e secondo correttezza;
- ad effettuare le operazioni di trattamento di cui all’art. 4, Paragrafo 1, n. 2 del RGPD per lo svolgimento delle funzioni istituzionali di competenza della Commissione giudicatrice;
- ad accedere unicamente alle banche dati strettamente necessarie per l’espletamento delle funzioni istituzionali proprie dei procedimenti di competenza della Commissione giudicatrice.

Il componente della Commissisone giudicatrice, individuato quale Incaricato al trattamento dei dati deve:

- per l’accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali personali di accesso, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati o non consentiti e di rendere possibile, in qualunque momento, l’individuazione dell’autore materiale del trattamento;
- conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- mantenere la massima riservatezza ed il dovuto riserbo sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali con riferimento alla gestione dei procedimenti amministrativi di competenza della Commissione giudicatrice;
- custodire e controllare i dati personali affidati affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile del trattamento dei dati;
- conservare i dati rispettando le misure di sicurezza predisposte dall’Ente;
- fornire al Responsabile del trattamento dei dati tutte le informazioni relative all’attività svolta, al fine di consentire una efficace attività di controllo.

Con riferimento all’utilizzo della postazione di lavoro assegnata in uso:

- Il Personal Computer (PC) affidato al componente della Commissione giudicatrice è uno strumento di lavoro. Ogni utilizzo non inerente l’attività lavorativa può contribuire ad innescare disservizi, costi ulteriori di manutenzione e minacce alla sicurezza dei dati personali trattati dall’Ente.
- Il componente della Commissione giudicatrice deve custodire la propria strumentazione in modo diligente, segnalando con tempestività ogni danneggiamento, avaria, furto o smarrimento al proprio Responsabile del trattamento.
- L’accesso a ciascun PC è protetto da credenziale di autenticazione costituita da una User ID (codice per l’identificazione dell’autorizzato) associata a una PASSWORD riservata (parola chiave), conosciuta esclusivamente dal medesimo autorizzato.
- Gli Autorizzati del trattamento dei dati sono responsabili della custodia e dell’utilizzo diligente e consapevole delle proprie credenziali di autenticazione.
- Non è consentito installare autonomamente programmi provenienti dall’esterno senza la preventiva autorizzazione del Responsabile del trattamento e dell’Amministratore di Sistema dell’Ente.
- Non è consentito modificare le caratteristiche impostate sui PC assegnati, le configurazioni della rete LAN presente nella sede dell’Ente e la configurazione del Browser per la navigazione, salvo esplicita autorizzazione dell’Amministratore di Sistema dell’Ente.
- Non è consentita l’installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro se non con l’espressa autorizzazione del Responsabile del trattamento dei dati e dell’Amministratore di Sistema dell’Ente. Si deve prestare la massima attenzione ai supporti di memorizzazione di origine esterna, avvertendo senza indugio il Responsabile del trattamento dei dati e l’Amministratore di Sistema nel caso in cui si dovesse rilevare la presenza di virus.
- E’ vietato utilizzare gli strumenti informatici dell’Amministrazione al fine di custodire, far circolare ovvero promuovere, materiale pubblicitario personale, codice maligno (virus, trojan horses, programmi non licenziati) e ogni altra tipologia di materiale non autorizzato.
- E’ vietato copiare, scaricare ovvero mettere a disposizione di altri materiale protetto dalla legge sul diritto di autore (documenti, files musicali, film e filmati) di cui l’Ente non abbia acquisito i diritti.
- E’ vietato rimuovere, danneggiare deliberatamente ovvero asportare componenti hardware.
- Al Commissario al quale sia stato assegnato dall’Amministrazione un elaboratore portatile, è responsabile dello stesso e deve custodirlo con diligenza sia durante gli spostamenti che durante l’utilizzo nel luogo di lavoro.
- Ai PC portatili si applicano le stesse regole di utilizzo previste per i PC fissi connessi in Rete.

Con riferimento al collegamento ad Internet

- E’ vietato l’accesso e l’utilizzo delle risorse di rete in assenza di preventiva autenticazione informatica da parte dell’Unità di Elaborazione allo scopo preposta.
- E’ vietato l’utilizzo di modem per l’accesso ad Internet, salvo specifica autorizzazione in tal senso da parte del Responsabile del trattamento e dell’Amministratore di Sistema dell’Ente.
- Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all’interno dell’Ente.
- Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento dell’ attività istituzionale. E’ proibita la navigazione in Internet per motivi diversi da quelli funzionali all’attività lavorativa stessa.
- Ciascun dipendente è direttamente e personalmente responsabile dell’uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
- E’ tassativamente vietata l’effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili salvo i casi espressamente autorizzati o attinenti ai compiti ed alle mansioni assegnate e con il rispetto delle normali procedure di acquisto.
- E’ vietata ogni forma di registrazione a siti o a mailing list i cui contenuti non siano legati allo svolgimento dell’attività di Commissario di gara.
- E’ vietata la partecipazione a Forum, l’utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (ovvero nicknames) se non strettamente attinenti l’attività lavorativa svolta.
- E’ vietata tassativamente la navigazione in siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche e sindacali o le abitudini sessuali dell’utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti oltraggiosi, discriminatori ovvero che offendono il comune senso del pudore.

Al componente della Commissione non è consentito:

- servirsi o dar modo ad altri di servirsi della stazione di accesso ad Internet per attività non istituzionali, per attività poste in essere in violazione del diritto d’autore o altri diritti tutelati dalla normativa vigente;
- scaricare software dalla rete se non espressamente autorizzato dal Responsabile del trattamento e dall’Amministratore di Sistema dell’Ente;
- utilizzare internet provider diversi da quello ufficiale dell’Ente e connettere stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dalla presente Determinazione e dalle leggi penali, civili e amministrative in materia di disciplina dell’attività e dei servizi svolti sulla rete.

Con riferimento all’utilizzo dei Supporti Magnetici o Ottici

- non è consentito scaricare files (programmi, archivi di dati, ecc) contenuti in supporti magnetici e/o ottici che non abbiano attinenza con la propria prestazione lavorativa;
- è fatto obbligo di sottoporre a controllo preventivo tutti i files di provenienza incerta o esterna, attinenti l’attività lavorativa.

ISTRUZIONE OPERATIVA DATA BREACH

L’art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all’autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.
L’obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all’interessato.
Per **“Violazione di dati**” si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

Cosa è una violazione dei dati personali (data breach)?

Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.
Una violazione dei dati personali può compromettere la riservatezza, l’integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l’accesso o l’acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l’impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Cosa fare in caso di violazione dei dati personali?
Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile**che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.
Il responsabile del trattamento e/o persona autorizzata o designata dal titolare che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare E IL DPO in modo che possano attivarsi.
Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere **accompagnate dai motivi del ritardo.**
Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l’impatto.
Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all’Autorità di effettuare eventuali verifiche sul rispetto della normativa.

Che tipo di violazioni di dati personali vanno notificate?
Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.
Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

Luogo e Data

Il Soggetto designato attuatore
Il Dirigente
Ing. Filippo Cangialosi

Per presa visione e accettazione della presente:
Dott. …….