DETERMINA 2541 DEL 14/06/2022

OGGETTO: PNRR - M5 - C2 - I 2.3 PROGRAMMA INNOVATIVO NAZIONALE PER LA QUALITÀ DELL'ABITARE – PINQUA ID. 9, ID. 309 - NOMINA RESPONSABILE DEL TRATTAMENTO AI SENSI DELL'ART. 28 DEL REGOLAMENTO (UE) 679/2016

Il Dirigente della Direzione
Lavori Pubblici Responsabile Programma Triennale Amministrativo Lavori Pubblici Estimo

Premesso che:

- al fine di dare attuazione agli interventi PNRR rientranti nell'ambito del PINQuA, il MIMS, quale "amministrazione centrale titolare dell'investimento" ha reso disponibile ai Soggetti Beneficiari e ai Soggetti Attuatori il supporto tecnico-operativo prestato da INVITALIA ai sensi dell'articolo 10 del decreto legge n. 77/2021 convertito dalla legge n. 108/2021 e nell'ambito di quanto previsto dalla Circolare del Ministero dell'Economia e Finanze - Ragioneria Generale dello Stato del 24 gennaio 2022, n. 6;
- l'Amministrazione comunale ha stabilito di avvalersi di INVITALIA come Centrale di Committenza, ai sensi degli articoli 37, co. 7, lett. b), e 38 del decreto legislativo del 18 aprile 2016, n. 50;
- la predetta Società sta procedendo per conto del Comune di Verona, all'indizione, gestione e aggiudicazione delle necessarie procedure d'appalto pubblicate sulla piattaforma e-procurement *InGaTe Invitalia Gare Telematiche* per la conclusione dei seguenti Accordi Quadro:

  AQ.1 - per l'affidamento di lavori (OG1 – OG11) e servizi di ingegneria e architettura (E.21 – E.06 – S.03 – IA.02 – IA.04) per la nuova edificazione, ristrutturazione e riqualificazione di edifici pubblici residenziali e non;

  AQ.2 - per l'affidamento di lavori (OG2 – OG11) e servizi di ingegneria e architettura (E.22 – E.06 – S.03 – IA.02 – IA.04) per restauro, riqualificazione e manutenzione di immobili pubblici sottoposti a tutela;

  AQ.3 - per l'affidamento di lavori (OG3) e servizi di ingegneria e architettura (V.02 – E.19 – S.04) per la realizzazione di interventi afferenti alla mobilità, inclusa quella ciclabile;

  AQ.4 - per l'affidamento di lavori (OS24) e servizi di ingegneria e architettura (E.19) per la rigenerazione di aree e spazi pubblici;

- con determinazione n. 2181 del 19 maggio 2022 del Direttore Area Lavori Pubblici all'epoca in servizio - Referente per il Comune di Verona per le procedure in questione, si è provveduto a nominare Invitalia SpA quale Responsabile del Trattamento ai sensi

e per gli effetti dell'art. 28 del regolamento (UE) 679/2016, esclusivamente per le procedure AQ1 e AQ2;

Considerato che titolare del trattamento dei dati è il Comune di Verona e, pertanto risulta opportuno riunire in un unico atto le nomine a Responsabile del trattamento per tutte le suindicate procedure AQ1 - AQ2 - AQ3 – AQ4;

Ritenuto, pertanto, di revocare la suindicata determinazione e 2181/2022 e di provvedere come indicato nella parte dispositiva del presente provvedimento;

Visti gli artt. n. 107 e n. 124 del decreto legislativo n. 267/2000 e successive modificazioni;

DETERMINA

1. di revocare, per le ragioni indicate in premessa, la determinazione n. 2181 del 19 maggio 2022;

2. di nominare, sempre per le ragioni sopraindicate, Invitalia - Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa SpA con sede in via Calabria, 46 – 00187 Roma, Responsabile del Trattamento dei dati personali, ai sensi e per gli effetti dell'art. 28 del regolamento (UE) 679/2016, per tutte le procedure AQ1 - AQ2 - AQ3- AQ4, indicate in premessa, alle condizioni tutte previste nell'allegato accordo di nomina, che contestualmente si approva e che sarà sottoscritto tra le parti;

3. il presente provvedimento sarà pubblicato all'Albo Pretorio on line ai sensi dell'art. 124 del succitato decreto legislativo n. 267/2000.

Firmato digitalmente da:
Il Dirigente
GIANLUCA FELICI

INVITALIA

Agenzia nazionale per l'attrazione
degli investimenti e lo sviluppo d'impresa SpA

Documento di sintesi delle misure tecniche e organizzative di INVITALIA S.P.A.

Via Calabria, 46 00187 Roma
T +39 06 421 601 F +39 06 421 606 16
www.invitalia.it

Azionista unico Ministero dell'Economia
e delle Finanze
Capitale sociale € 836.383.864,02

Iscritta al Registro delle Imprese di Roma
P.IVA e C.F. 05678721001

1. Scopo e contesto

Il presente documento descrive le misure tecniche e organizzative relative alla sicurezza e al sistema dei controlli messi in atto da INVITALIA, quale responsabile del trattamento, nella gestione delle attività che afferiscono a una convenzione o contratto con committente esterno.

Per "committente" si deve intendere ogni utilizzatore dei servizi offerti da INVITALIA per la realizzazione delle attività proprie e/o strumentali al perseguimento delle finalità pubbliche degli stessi committenti.

Con riferimento alle operazioni di trattamento operate nell'ambito dell'Agenzia, è necessario effettuare una partizione, tenuto conto del ruolo, delle attività e dei compiti istituzionali affidati alla medesima:

1. trattamenti dei dati personali operati da Invitalia in qualità di Titolare, per lo svolgimento della propria attività istituzionale e in conformità a specifiche disposizioni normative e/o regolamentari, nonché per adempiere agli obblighi legali, fiscali, contabili e contrattuali tipici di una società. In tale contesto, vanno anche evidenziati gli obblighi a cui l'Agenzia è soggetta per essere sottoposta al controllo della Corte dei Conti ed al rispetto della normativa in tema di trasparenza e anticorruzione, tipiche degli organismi pubblici;
2. trattamenti dei dati personali operati dalle Pubbliche Amministrazioni, in conformità ai rispettivi fini istituzionali, nonché a specifiche disposizioni normative e/o regolamentari. In tale ambito, Invitalia agisce per supportare le Pubbliche Amministrazioni nello svolgimento delle attività tecniche, economiche e finanziarie richieste, anche agendo direttamente quale Centrale di Committenza o Stazione Appaltante e quale società in house ai sensi dell'art. 192, co. 1 del D.Lgs. 50/2016, nonché per fornire supporto nella progettazione e attivazione dei programmi finanziati con fondi comunitari e nazionali. Le operazioni di trattamento svolte da INVITALIA, anche unitamente ad altro Titolare, sono consentite per lo svolgimento delle funzioni istituzionali proprie delle Amministrazioni e per adempiere a specifiche disposizioni normative e regolamentari sia nazionali che comunitarie, nel pieno rispetto della disciplina in materia di protezione dei dati personali.

INVITALIA monitora, modifca ed aggiorna le misure di sicurezza indicate nel presente documento per adattarsi agli standard di sicurezza in continua evoluzione e, ove necessario, verrà data comunicazione di tali modifiche ai committenti.

1.1. Descrizione generale delle misure di sicurezza tecniche e organizzative

INVITALIA ha adottato un Sistema di Gestione Privacy, contenuto nel documento denominato "Gestione del Sistema Privacy - AG-SP-MANPR - Manuale di Sistema" che descrive il Sistema Privacy di Invitalia e l'insieme delle procedure, delle istruzioni operative e della modulistica approntate in relazione ai trattamenti dei dati personali eseguiti nel rispetto del Regolamento (UE) 2016/679 (GDPR), nonché degli ulteriori provvedimenti applicabili in materia di protezione dei dati personali. Il Sistema di Gestione Privacy definisce altresì i ruoli privacy con l'indicazione dei compiti e delle funzioni relative alla gestione dei dati.

In seguito alla valutazione dei trattamenti svolti da INVITALIA, si è ritenuto di rientrare in ipotesi di obbligatorietà della nomina del DPO – Data protectione Officer ed è stato costituito un Ufficio privacy e team DPO interno all'Agenzia.

Nell'ambito del Sistema Gestione Privacy è prevista una sezione dedicata all'Analisi dei rischi relativi ai trattamenti effettuati dall'Agenzia, che viene svolta con cadenza almeno annuale e alla DPIA - Valutazione d'impatto sulla protezione dei dati.

Le misure di sicurezza, tecniche e organizzative, adottate da Invitalia garantiscono un livello di sicurezza adeguato al rischio individuato e sono volte a proteggere le informazioni aziendali dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione e da accessi non autorizzati, nonché da trattamenti non consentiti o non conformi rispetto alla finalità per cui le stesse sono state raccolte. Tali misure sono volte ad assicurare, su base permanente, la riservatezza e l'integrità delle informazioni, nonché la disponibilità e la resilienza dei sistemi e dei trattamenti ivi operati, in conformità alla normativa applicabile.

Le misure di sicurezza sono state adottate in funzione dei rischi identificati e analizzati nell'ambito della struttura organizzativa e del loro impatto sulle risorse dei sistemi, sulle infrastrutture e sui dati ivi trattati, come da "Analisi dei rischi" che viene eseguita con cadenza almeno annuale.

Invitalia, a seguito dell'attività di risk assessment condotta periodicamente, provvede ad effettuare la DPIA in relazione ai trattamenti che presentavano rischi elevati, in conformità alle prescrizioni normative. Le DPIA sono conservate dal DPO e dal suo team.

Il Sistema privacy di Invitalia, per quanto riguarda gli aspetti relativi alla gestione della sicurezza delle informazioni, si completa, dal punto di vista sia tecnico che organizzativo, nel "Manuale di Sistema – Sistema di gestione dell'Information Technology – GR-SIN-MANSGIT" e suoi allegati, pubblicato sull'intranet aziendale.

2. Misure organizzative per la sicurezza delle informazioni

Obiettivo:

Descrivere la struttura e i processi organizzativi adottati da INVITALIA per garantire la sicurezza delle informazioni e dei dati oggetto di trattamento.

Misure:

a. INVITALIA, nell'ambito del Modello di Organizzazione, Gestione e Controllo adottato ai sensi del Dlgs 231/01, ha introdotto ed adottato un "Sistema di gestione privacy" composto da policy e direttive in materia di protezione dei dati personali, approvate dalla dirigenza e diffuse a tutto il personale, mediante la pubblicazione sull'intranet aziendale;

b. Invitalia procede periodicamente alle attività di rilevazione e mappatura dei trattamenti operati nell'ambito delle proprie Funzioni, al fine di aggiornare i trattamenti già censiti, verificandone la correttezza e la rispondenza alla realtà aziendale, nonché per rilevare eventuali nuove operazioni di trattamento nel rispetto delle procedure aziendali;

c. l'attività di mappatura consente, altresì, di aggiornare e/o integrare tutte le informazioni necessarie per permettere di assolvere agli obblighi previsti dalla normativa vigente in materia di protezione dei dati personali con riguardo ai ruoli privacy, alla redazione di ulteriori istruzioni, all'implementazione delle misure di sicurezza e di quant'altro necessario per adempiere agli obblighi normativi e adeguare costantemente il Sistema Privacy dell'Agenzia;

d. la mappatura dei trattamenti effettuati da Invitalia è riportata nei Registri delle attività di trattamento ai sensi dell'art. 30 del GDPR;

e. INVITALIA ha elaborato un Organigramma Privacy, in virtù del quale sono stati definiti ruoli e responsabilità del personale dipendente, che è stato autorizzato al trattamento dei dati;

f. il personale INVITALIA è inoltre vincolato alla riservatezza e al rispetto del Codice etico adottato ai sensi della L. 231/01;

g. INVITALIA utilizza ISMS (Information Security Management Systems) quale fondamento delle proprie pratiche di sicurezza delle informazioni;

h. ogni ISMS è stata e continua ad essere verificata da un auditor esterno e indipendente;

i. INVITALIA ha adottato, nell'ambito del Sistema di Gestione dell'Information Technology, una policy per la gestione dei rischi IT, denominata "IT Risk Management - GR-PY-SIN-ITRM -policy", pubblicata sull'intranet aziendale.

3. Misure tecniche per la sicurezza delle informazioni

3.1. Sistema di Accesso

Obiettivo:

Proteggere lo strumento nel quale sono contenuti i dati personali che Invitalia tratta per conto del Committente, garantire che i sistemi contenenti i dati vengano utilizzati solo da utenti autorizzati e autenticati, e assicurare che il personale autorizzato ad utilizzare i sistemi acceda solo ai dati per cui è autorizzato.

Misure:

a. Il servizio di INVITALIA opera su infrastruttura erogata attraverso fornitori di servizi cloud pubblici. Questi sono protetti da un definito e protetto perimetro fisico, elevati controlli fisici tra cui: meccanismi di accesso, controllo nelle zone di consegna e carico, sorveglianza e guardie di sicurezza;

b. i fornitori di servizi cloud pubblici sono selezionati sulla base di ristrettissimi vincoli di certificazione in conformità ai controlli di sicurezza INVITALIA. Le certificazioni richieste sono:
   - ISO/IEC 27018:2019: codice di condotta incentrato sulla protezione dei dati personali nel cloud.
   - Certificazione SOC 1 (almeno SSAE 16) Type 2
   - Certificazione SOC 2 Type 2
   - Certificazione SOC 3
   - Certificazione ISO/IEC 27001
   - Certificazione ISO/IEC 9001

c. l'accesso ai sistemi INVITALIA è garantito solo al personale INVITALIA. L'accesso è inoltre strettamente limitato a quanto necessario per l'espletamento delle proprie funzioni, sulla

base dei principi di "segregation of duties" e "need to know";

d. INVITALIA ha adottato una policy, pubblicata sull'intranet aziendale, per la gestione della dotazione al personale della strumentazione informatica aziendale, denominata "Gestione Dotazione Informatica Aziendale - GR-PY-SIN-GDII - Policy";

e. INVITALIA ha adottato un sistema di Identity Management per consentire agli amministratori IT di accedere ai sistemi IT autorizzati tramite il proprio account aziendale denominato (la loro identità digitale unica nell'azienda). Ogni sistema IT delega l'autenticazione di un utente denominato al sistema di messaggistica istantanea che fornisce sia l'autenticazione che l'autorizzazione per la risorsa richiesta/sistema IT;

f. tutti gli utenti accedono ai sistemi INVITALIA con un identificativo univoco (UID);

g. INVITALIA ha stabilito una Password Policy che proibisce di condividere le password ed esige che le password siano modificate regolarmente e le password predefinite alterate. Tutte le password devono rispettare dei requisiti minimi di complessità e diversità dalle precedenti e vengono conservate in forma criptata;

h. l'accesso ai sistemi contenenti i dati viene consentito attraverso un tunnel VPN sicuro e richiede un secondo fattore di autenticazione;

i. INVITALIA ha un processo completo per disattivare gli utenti e il loro accesso, quando il personale lascia l'azienda o una particolare funzione;

j. tutti gli accessi o i tentativi di accesso ai sistemi vengono registrati e monitorati;

k. INVITALIA restringe l'accesso del personale ai soli dati di cui necessita ("need-to-know basis") per svolgere il servizio per conto del committente;

l. INVITALIA ha adottato un'istruzone operativa, pubblicata sull'intranet aziendale, che descrive il processo di registrazione e conservazione dei file di log di sistema effettuati sui sistemi ed applicativi di INVITALIA, denominata "Gestone dei Log di Sistema - GR-IO-SIN-GLS - Istruzione operativa".

4. Trasmissione/archiviazione/distruzione dei dati

Obiettivo:

Assicurare che i dati non siano letti, copiati, alterati o cancellati da soggetti non autorizzati durante il trasferimento, l'archiviazione o la distruzione.

Misure:

a. L'accesso dei committenti e del personale degli stessi ai portali del servizio INVITALIA è protetto da una versione sicura di Transport Layer Security (TLS 1.2);

b. INVITALIA crittografa tutti i dati conservati nei dispositivi di memoria per l'archiviazione dei dati all'interno dei data center di produzione, utilizzando misure di Strong Encryption (AES 256);

c. l'accesso ai data center, dove i dati sono conservati, avviene attraverso un tunnel VPN (IPSEC) e richiede molteplici fattori di autenticazione;

d. a seconda delle preferenze indicate e conformemente ai termini del contratto stipulato con il committente, quando viene chiusa l'istanza del committente titolare dell'account, INVITALIA restituisce e/o elimina i dati personali alla cessazione del contratto;

e. pseudonimizzazione / anonimizzazione – Dove la cancellazione dei record non è possibile a causa dell'integrità referenziale, l'anonimizzazione consiste nell'oscurare i dati in modo tale che non siano recuperabili;

f. in caso di dismissione, le apparecchiature o i dischi che contengono i dati personali del cliente vengono distrutti in modo sicuro e viene rilasciata una certificazione di avvenuta distruzione.

5. Riservatezza e integrità

Obiettivo:

Garantire che i dati rimangano confidenziali, intatti, completi e aggiornati durante il trattamento.

Misure:

a. INVITALIA forma il suo personale coinvolto nello sviluppo o nei test dei software sulle procedure di sicurezza delle applicazioni e nelle procedure di sicurezza dei codici;

b. INVITALIA possiede un archivio centrale protetto che conserva il codice sorgente del prodotto e il cui accesso è strettamente riservato al solo personale autorizzato;

c. INVITALIA possiede un programma formale di sicurezza delle applicazioni e impiega un processo di sviluppo del software (Software Development Lifecycle - SDLC) sicuro e robusto;

d. i test di sicurezza includono la revisione del codice, i test di penetrazione e strumenti di analisi su base periodica del codice al fine di individuare eventuali difetti;

e. tutte le modifiche ai sistemi inerenti il servizio di INVITALIA avvengono attraverso un meccanismo di rilascio approvato, rientrante in un programma formale di controllo delle modifiche.

6. Disponibilità e Resilienza

Obiettivo:

Garantire che i dati siano protetti dalla distruzione o perdita accidentale e che in caso di incidente di servizio avvenga tempestivamente l'accesso, il ripristino o la disponibilità dei dati.

Misure:

a. INVITALIA utilizza un elevato livello di ridondanza durante l'archiviazione dei dati. I dati che Invitalia tratta per conto dei Committenti vengono archiviati in triplice copia (principale, standby locale e remoto) in due data center geograficamente separati;

b. l'infrastruttura erogata dai cloud service provider è ridondante su più zone di disponibilità e con più interconnessioni per garantire che non ci sia alcun punto di errore unico al loro interno;

c. al fine di proteggere i i dati da distruzioni accidentali e perdite, i dati vengono a loro volta sottoposti a backup su servizi di storage account a loro volta ridondati con indice di disponibilità al 99,9999%;

d. ogni data center dispone di più punti di accesso a Internet per salvaguardare la connettività;

e. INVITALIA ha adottato una procedura volta ad assicurare una corretta definizione, esecuzione e gestione delle attività di back up e restore dei dati, denominata "Backup & Restore - GR-IO-SIN-BARE - istruzione operativa", pubblicata sull'intranet aziendale.

7. Separazione dei Dati

Obiettivo:

Per garantire che i dati di ogni committente siano trattati separatamente.

Misure:

a. INVITALIA ricorre, al minimo, alla separazione logica all'interno della propria infrastruttura al fine di separare i dati dei committenti;

b. INVITALIA mantiene ambienti separati gli ambienti di sviluppo, test/QA, test di integrazione utente e ambienti di produzione.

8. Gestione degli incidenti – Data Breach

Obiettivo:

In caso di Data Breach, l'incidente viene gestito prontamente e le conseguenze della violazione sono ridotte al minimo, grazie alle azioni che vengono poste in essere e il Committente viene informato non appena INVITALIA venga a conoscenza della violazione.

Misure:

a. INVITALIA ha adottato una procedura organizzativa per la gestione delle violazioni e la relativa notifica all'Autorità Garante e, ove necessario, agli Interessati denominata denominata "Gestione

delle violazioni di dati personali - AG-GESVIOL - Procedura organizzativa" e pubblicata sull'intranet aziendale;

b. INVITALIA ha adottato una procedura organizzativa che descrive le attività necessarie a definire i processi di gestione degli incidenti e dei problemi IT, di analizzarne le cause assicuranedone la risoluzione tempestiva, verificando che ogni richiesta di intervento sia: classificata per grado di importanza, documentata, monitorata e risolta, denominata "Incident & Problem Management -GR-SIN-IPMGMT- procedura organizzativa", pubblicata sull'intranet aziendale.

9. Sub fornitori

Obiettivo:

Garantire che i fornitori di servizi di cui si avvale INVITALIA, nella veste di titolare e/o responsabile del trattamento, proteggano e gestiscano tutti i dati personali a cui accedono in conformità: (i) agli standard di sicurezza di INVITALIA, (ii) alla normativa vigente in materia di protezione dei dati personali e (iii) ai requisiti stabiliti nei modelli contrattuali e nelle condizioni generali di contratto sottoposti ai soggetti terzi.

Misure:

a. Sono state classificate delle categorie di attività e di conseguenza di dati che possono essere oggetto di trattamento da parte di un fornitore e che tale trattamento, effettuato per conto del titolare e/o del responsabile, comporti l'individuazione del fornitore quale Responsabile del trattamento ex art. 28 GDPR;

b. al fornitore che tratta dati per conto di INVITALIA, viene sottoposto un accordo sul trattamento (data processing agreement) ai sensi dell'art. 28 GDPR;

c. come indicato nelle procedure e policy aziendali relative ai processi di acquisto e scelta del foritore, nonché nel Sistema di Gestione Privacy, INVITALIA ricorre a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti stabiliti dalla normativa e garantisca la tutela dei diritti dell'interessato;

d. vengono eseguiti audit periodici per verificare e valutare le garanzie del fornitore per le attvità che comportano un trattamento di dati per conto di INVITALIA.

Roma, 29/11/2021

Il DPO
Dr. Francesco Sprovieri

Sistemi Informativi
Dr. Alessio Antolini

PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR)

MISSIONE M5 - COMPONENTE C2 - AMBITO INTERVENTO/MISURA 2 - INVESTIMENTO 2.3

PROGRAMMA INNOVATIVO NAZIONALE PER LA QUALITÀ DELL'ABITARE – PINQuA - [M5C2I2.3]

- **Obiettivo T1/2026:** Entro primo trimestre 2026 sostegno a *10.000 unità abitative* (in termini sia di costruzione che di riqualificazione). Il conseguimento soddisfacente dell'obiettivo dipende anche dal conseguimento soddisfacente di un obiettivo secondario che copra almeno *800.000 metri quadrati di spazi pubblici*.

ACCORDO DI NOMINA A RESPONSABILE DEL TRATTAMENTO
ai sensi e per gli effetti dell'art. 28 del Regolamento (UE) 679/2016

AQ.1	PNRR – MISSIONE M5 - COMPONENTE C2 - INVESTIMENTO 2.3 - PROGRAMMA INNOVATIVO NAZIONALE PER LA QUALITÀ DELL'ABITARE (PINQuA) – PROCEDURA DI GARA APERTA AI SENSI DEGLI ARTT. 54 E 60 DEL D.LGS N. 50/2016, DA REALIZZARSI MEDIANTE PIATTAFORMA TELEMATICA, PER LA CONCLUSIONE DI ACCORDI QUADRO CON PIÙ OPERATORI ECONOMICI PER L'AFFIDAMENTO DI LAVORI (**OG1 – OG11**) E SERVIZI DI INGEGNERIA E ARCHITETTURA (**E.21 – E.06 – S.03 – IA.02 – IA.04**) PER LA **NUOVA EDIFICAZIONE, RISTRUTTURAZIONE E RIQUALIFICAZIONE DI EDIFICI PUBBLICI RESIDENZIALI E NON**.
AQ.2	PNRR – MISSIONE M5 - COMPONENTE C2 - INVESTIMENTO 2.3 - PROGRAMMA INNOVATIVO NAZIONALE PER LA QUALITÀ DELL'ABITARE (PINQuA) – PROCEDURA DI GARA APERTA AI SENSI DEGLI ARTT. 54, 60 E 145 DEL D.LGS N. 50/2016, DA REALIZZARSI MEDIANTE PIATTAFORMA TELEMATICA, PER LA CONCLUSIONE DI ACCORDI QUADRO CON PIÙ OPERATORI ECONOMICI PER L'AFFIDAMENTO DI LAVORI (**OG2 – OG11**) E SERVIZI DI INGEGNERIA E ARCHITETTURA (**E.22 – E.06 – S.03 – IA.02 – IA.04**) PER **RESTAURO, RIQUALIFICAZIONE E MANUTENZIONE DI IMMOBILI PUBBLICI SOTTOPOSTI A TUTELA**.
AQ.3	PNRR – MISSIONE M5 - COMPONENTE C2 - INVESTIMENTO 2.3 - PROGRAMMA INNOVATIVO NAZIONALE PER LA QUALITÀ DELL'ABITARE (PINQuA) – PPROCEDURA DI GARA APERTA AI SENSI DEGLI ARTT. 54 E 60 DEL D.LGS. N. 50/2016, DA REALIZZARSI MEDIANTE PIATTAFORMA TELEMATICA, PER LA CONCLUSIONE DI ACCORDI QUADRO CON PIÙ OPERATORI ECONOMICI PER L'AFFIDAMENTO DI LAVORI (**OG3**) E SERVIZI DI INGEGNERIA E ARCHITETTURA (**V.02 – E.19 – S.04**) PER LA **REALIZZAZIONE DI INTERVENTI AFFERENTI ALLA MOBILITÀ, INCLUSA QUELLA CICLABILE**.
AQ.4	PNRR – MISSIONE M5 - COMPONENTE C2 - INVESTIMENTO 2.3 - PROGRAMMA INNOVATIVO NAZIONALE PER LA QUALITÀ DELL'ABITARE (PINQuA) – PROCEDURA DI GARA APERTA AI SENSI DEGLI ARTT. 54 E 60 NONCHÈ, SE DEL CASO, DELL'ART. 145 DEL D.LGS N. 50/2016, DA REALIZZARSI MEDIANTE PIATTAFORMA TELEMATICA, PER LA CONCLUSIONE DI ACCORDI QUADRO CON PIÙ OPERATORI ECONOMICI PER L'AFFIDAMENTO DI LAVORI (**OS24**) E SERVIZI DI INGEGNERIA E ARCHITETTURA (**E.19**) PER LA **RIGENERAZIONE DI AREE E SPAZI PUBBLICI**.

Il Titolare del trattamento è

Comune di Verona in persona del legale rappresentante *pro tempore*:

- considerata l'entrata in vigore del nuovo Regolamento (UE) 679/2016 del Parlamento europeo

e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito, "***GDPR***") pubblicato sulla Gazzetta ufficiale dell'unione europea il 04 maggio 2016;

- preso atto che l'art. 4, n. 8 del GDPR definisce il "Responsabile" come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- considerato che il decreto legislativo 14 agosto 2013, n. 93 contempla le violazioni Privacy anche nell'ambito della responsabilità amministrativa dell'ente a norma del decreto legislativo 8 giugno 2001, n. 231;
- tenuto conto che il GDPR dispone che il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
- considerato che il Responsabile ha adottato le misure di sicurezza tecniche e organizzative ai sensi della ISO 27001, come previste dal GDPR, **il cui documento di sintesi si allega al presente Accordo;**
- rilevato che i compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare e che il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al GDPR e delle proprie istruzioni;
- ritenuto che Invitalia - Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa S.p.A. (di seguito, "***Invitalia***"), per l'ambito di attribuzioni, funzioni e competenze, conferite mediante la Determinazione a contrarre prot. n. 0093861, che qui si intende integralmente richiamata, possiede i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza;
- tenuto conto che l'Informativa in materia di protezione dei dati personali ai sensi degli Artt. 13 e 14 del Regolamento (UE) 2016/679 (GDPR), rilasciata dal Titolare del trattamento, con riferimento alle **procedure per la conclusione degli AQ.1, AQ.2, AQ.3 e AQ.4** , è resa disponibile sul portale web del Comune di Verona al seguente link: *https://www.comune.verona.it/nqcontent.cfm?a_id=81377*
- **nell'ambito delle procedure in epigrafe selezionate,**

Tutto ciò premesso, il Titolare

NOMINA

Invitalia, con sede in Roma via Calabria, 46, che accetta, quale "Responsabile del Trattamento" ai sensi e per gli effetti dell'art. 28 del Regolamento (UE) 679/2016, con riferimento alle prestazioni di cui alla citata Determinazione a contrarre, nell'ambito delle funzioni di Centrale di Committenza, ai sensi del combinato disposto dell'art. 3, co. 1, lett. l), n. 2), dell'art. 37, co. 6 e 7, lett. b), e dell'art. 38, co. 1, del decreto legislativo 18 aprile 2016, n. 50 (Codice dei Contratti), per la procedura/e selezionata/e in epigrafe.

In qualità di Responsabile del trattamento dei dati, Invitalia è consapevole di avere il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le seguenti istruzioni impartite dal Titolare.

Il Responsabile del trattamento si impegna, entro e non oltre 30 gg. dalla data di sottoscrizione ed

accettazione della presente nomina, ad impartire per iscritto ai propri soggetti autorizzati del trattamento, istruzioni in merito alle operazioni di trattamento dei dati personali ed a vigilare sulla loro puntuale applicazione.

Le parti, come sopra individuate convengono e stipulano quanto segue: le premesse di cui sopra costituiscono parte integrante del presente atto.

1. Finalità e modalità del trattamento

Ai sensi del considerando n. 81 e dell'art. 28 del GDPR il trattamento svolto dal Responsabile in questo atto designato deve essere effettuato per conto del titolare del trattamento che è l'unico soggetto abilitato a individuare le finalità e le modalità del trattamento affidato al Responsabile.

In virtù di ciò il Responsabile garantisce di poter far valere garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

2. Sub-responsabile

Il Titolare autorizza il Responsabile del trattamento a ricorrere a un altro Responsabile del trattamento (subresponsabile) per l'esecuzione di specifiche attività di trattamento per conto del Titolare, sul sub-Responsabile del trattamento sono imposti dal primo Responsabile, mediante un contratto o un altro atto giuridico a norma del diritto dell'unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR.

3. Durata del trattamento

La durata del trattamento è prevista per tutta la durata dell'incarico conferito dal Titolare per le sole finalità connesse al pieno assolvimento degli obblighi previsti dalla procedura/e selezionata/e in epigrafe e dalla citata Determinazione a contrarre.

4. Diritti e obblighi del responsabile del trattamento

Quanto ai diritti ed obblighi del Responsabile in particolare si prevede che il Responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'art. 32 GDPR;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 GDPR per ricorrere ad un altro Responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare

l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR;

f) assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, vale a dire in relazione alla sicurezza del trattamento (art. 32), alla notifica di una violazione dei dati personali all'autorità di controllo (*data breach* di cui all'art. 33), alla comunicazione di una violazione dei dati personali all'interessato (*data breach* di cui all'art. 34), alla valutazione d'impatto sulla protezione dei dati (DPIA ex art. 35) e alla consultazione preventiva (art. 36), tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento;

g) su scelta del Titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi in materia di protezione dei dati personali e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;

i) con riguardo alle istruzioni impartite dal Titolare, il Responsabile del trattamento informi immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'unione, relative alla protezione dei dati.

5. Adesione a codici di condotta o meccanismi di certificazione

L'adesione da parte del Responsabile del trattamento a un codice di condotta approvato di cui all'art. 40 del GDPR o a un meccanismo di certificazione approvato di cui all'art. 42 del GDPR può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 dell'art. 28 GDPR.

6. Transizione da Responsabile a Titolare del trattamento

Fatti salvi gli articoli 82, 83 e 84 del GDPR, se il Responsabile del trattamento viola il GDPR, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione, ai sensi dell'art. 28, paragrafo 10, del GDPR.

7. Responsabilità

Il Responsabile è consapevole che ai sensi dell'art. 29 del GDPR egli, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'unione o degli Stati membri.

8. Registro del trattamento

In ottemperanza all'art. 30 del GDPR il Responsabile si impegna a tenere un registro in forma scritta, anche in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati (DPO);

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, paragrafo 1.

****

COMPITI E ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI IN APPLICAZIONE DELL'ART. 28 DEL REGOLAMENTO (UE) 679/2016

PRINCIPI GENERALI DA OSSERVARE

Ai sensi dell'art. 5 del GDPR, che stabilisce i "Principi applicabili al trattamento di dati personali", per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti nel trattamento affinché i dati siano sempre:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1 GDPR, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, paragrafo 1 GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»);

g) ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di illecita conoscibilità dei dati da parte di terzi;

h) se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal GDPR è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del

medesimo trattamento, ovvero alla cancellazione dei dati se non è possibile regolarizzare;

i) ciascun Responsabile deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni penali, civili ed amministrative;

l) in merito alla responsabilità civile si ricorda, relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, che, per evitare ogni responsabilità, l'operatore, anche nominato Responsabile, è tenuto a fornire la prova di avere applicato le misure tecniche e organizzative adeguate a garantire la sicurezza dei dati trattati.

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare:

- identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni: il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
- individuare le categorie dei trattamenti effettuati;
- individuare e regolamentare i trasferimenti di dati personali verso Paesi terzi;
- descrivere le misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;
- definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o la anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;
- adempiere agli obblighi di sicurezza: adottare, tramite il supporto tecnico degli amministratori di sistema, tutte le preventive misure di sicurezza, ritenute adeguate al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti al trattamento dei dati;
- assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- definire una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;
- far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti: in particolare, comunicare preventivamente al Titolare l'inizio di ogni trattamento che intende intraprendere autonomamente sui dati che gli siano stati affidati dal Titolare;
- segnalare al Titolare l'eventuale cessazione del trattamento;
- in merito ai soggetti autorizzati, il responsabile deve individuare, tra i propri lavoratori, designandoli per iscritto, le persone autorizzate al trattamento;
- recepire le istruzioni cui devono attenersi le persone autorizzate nel trattamento dei dati

impartite dal Titolare, assicurandosi che vengano materialmente consegnate agli stessi o siano già in loro possesso;

- adoperarsi al fine di rendere effettive le suddette istruzioni, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati e l'osservanza da parte delle persone autorizzate, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
- stabilire le modalità di accesso ai dati e l'organizzazione del lavoro da parte delle persone autorizzate, avendo cura di adottare preventivamente le misure tecniche ed organizzative adeguate e impartire le necessarie istruzioni ai fini del riscontro di eventuali richieste di esecuzione dei diritti da parte degli interessati.

ISTRUZIONI AL RESPONSABILE

Il Responsabile, sebbene non in via esaustiva, avrà i compiti e le istruzioni di seguito elencate, oltre agli ulteriori obblighi previsti dalla presente nomina.

Si ricorda che per ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:

a) il divieto di comunicazione o diffusione dei dati senza la preventiva autorizzazione del Titolare;

b) l'accesso ai dati è autorizzato limitatamente all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro, o, in casi eccezionali, quando si riceva espressa autorizzazione dal Titolare;

c) la fase di trattamento dei dati dovrà essere preceduta dalla informativa all'interessato (cliente/fornitore/dipendente/collaboratore) *ex* art. 14 del GDPR in forma scritta e dal consenso di questi al trattamento nei casi previsti dalla legge, fatti salvi diversi accordi contrattuali che prevedano l'informativa *ex* art. 13 del GDPR da parte del Titolare;

d) in caso di interruzione, anche temporanea, del lavoro predisporre il divieto a che i dati trattati non siano accessibili a terzi non autorizzati;

e) assicurarsi che le credenziali di autenticazione assegnate siano strettamente personali e rimangano riservate. Tali credenziali sono univocamente associate al soggetto autorizzato al quale sono state fornite;

f) gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati devono essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro;

g) qualsiasi altra istruzione può essere fornita dal Titolare che provvede, direttamente o a mezzo del Responsabile, a seconda di quanto contrattualmente previsto, anche alla formazione dei soggetti autorizzati.

TRATTAMENTO CONSENTITO

a) raccogliere, registrare e conservare i dati presenti negli atti e documenti su supporti cartacei o su supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

b) qualsiasi accesso e trattamento espressamente previsto dal profilo di autorizzazione associato alle mansioni inerenti il ruolo di Responsabile nell'ambito di attribuzioni, funzioni e competenze, conferite mediante la citata Determinazione a contrarre, che qui si intende integralmente richiamata;

c) qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di

quanto previsto dalla normativa in materia di tutela dei dati personali relativamente alle attività e al settore di competenza, come previsto dalla citata Determinazione a contrarre.

L'incarico di Responsabile del trattamento dei dati decade automaticamente alla scadenza o alla revoca dell'incarico.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali. una copia del presente atto di nomina dovrà essere restituita al Titolare, debitamente firmata per accettazione.

IL RESPONSABILE DICHIARA:

- di aver preso conoscenza dei compiti che gli sono affidati;
- di essere a conoscenza di quanto stabilito dal GDPR e dalla normativa in materia di tutela dei dati personali;
- di aver adottato tutte le misure le misure di sicurezza tecniche e organizzative ai sensi della ISO 27001, (GDPR), il cui documento di sintesi viene allegato al presente Accordo di nomina;
- di aver compreso e di attenersi alle Istruzioni dettate dal Titolare.

Verona,10 giugno 2022

IL TITOLARE DEL TRATTAMENTO

in persona del legale rappresentante pro tempore

Arch. Gianluca Felici
Dirigente Lavori Pubblici
Responsabile Programma Triennale
Amministrativo LLPP Estimo

_____

Per accettazione

IL RESPONSABILE DEL TRATTAMENTO

in persona del legale rappresentante pro tempore

_____

DOCUMENTAZIONE ALLEGATA

ALLEGATO A. **Documento di sintesi delle misure di sicurezza tecniche e organizzative di Invitalia S.P.A.**