COMUNE DI GENOVA

DIREZIONE IDROGEOLOGIA E GEOTECNICA, ESPROPRI, VALLATE

DETERMINAZIONE DIRIGENZIALE N. 2023-213.0.0.-82

L'anno 2023 il giorno 07 del mese di Luglio il sottoscritto Grassano Giorgio in qualita' di dirigente di Direzione Idrogeologia E Geotecnica, Espropri, Vallate, ha adottato la Determinazione Dirigenziale di seguito riportata.

OGGETTO: PRESA ATTO DEL PROTOCOLLO D'INTESA PER LA PROMOZIONE DI UNA COLLABORAZIONE SU TEMATICHE GEOTECNICHE TRA LA FONDAZIONE ISTITUTO ITALIANO DI TECNOLOGIA E IL COMUNE DI GENOVA

Adottata il 07/07/2023
Esecutiva dal 07/07/2023

07/07/2023	GRASSANO GIORGIO

Sottoscritto digitalmente dal Dirigente Responsabile

COMUNE DI GENOVA

DIREZIONE IDROGEOLOGIA E GEOTECNICA, ESPROPRI, VALLATE

DETERMINAZIONE DIRIGENZIALE N. 2023-213.0.0.-82

OGGETTO: PRESA ATTO DEL PROTOCOLLO D'INTESA PER LA PROMOZIONE DI UNA COLLABORAZIONE SU TEMATICHE GEOTECNICHE TRA LA FONDAZIONE ISTITUTO ITALIANO DI TECNOLOGIA E IL COMUNE DI GENOVA

IL DIRETTORE RESPONSABILE

Visti:

- il DECRETO LEGISLATIVO 18 agosto 2000, n. 267 "Testo unico delle leggi sull'ordina- mento degli enti locali" e, in particolare, l'art. 107 relativamente alle funzioni e responsabilità della dirigenza, nonché l'art. 192 in ordine alle determinazioni a contrarre e relative procedure;

- il DECRETO DEL PRESIDENTE DELLA REPUBBLICA 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" e ss. mm. ii.;

- il DECRETO LEGISLATIVO 30 marzo 2001, n. 165 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";

- lo Statuto del Comune di Genova approvato con Deliberazione del Consiglio Comunale del 12 giugno 2000, n. 72 e ss. mm. ii. e in particolare gli art. 77 e 80 i quali, in conformità ai principi dettati dalla Legge, disciplinano le funzioni ed i compiti della dirigenza;

- il vigente Regolamento di Contabilità approvato con deliberazione del Consiglio Comunale n. 34 del 04/03/1996 e ss. mm. ii. di cui, in ultimo, la modificazione con deliberazione del Consiglio Comunale n. 2 del 09/01/2018, ed in particolare l'art. 4 relativo alla competenza dei dirigenti responsabili dei servizi comunali.

Premesso che:

- il Comune di Genova, in sintonia in particolare con l'Assessore al Bilancio, Lavori Pubblici Opere strategiche infrastrutturali, Rapporti con i Municipi Pietro Piciocchi e il Consigliere delegato alle Vallate Alessio Bevilacqua, tramite la Direzione Idrogeologia e Geotecnica Espropri e

Vallate, sta perseguendo una politica di valorizzazione e riqualificazione delle vallate genovesi come tematica volta alla riappropriazione di una nostra identità culturale e finalizzata al ritorno dell'interesse culturale, economico sull'entroterra genovese in senso lato, esteso a tutta la Città Metropolitana e, anzi, sconfinando con le realtà di altre Regioni limitrofe, con cui è necessario dialogare per ricostituire un legame e un indotto, che attraverso la valorizzazione delle risorse paesaggistiche, storiche, economiche, possa indurre un ritorno all'insediamento e alla frequentazione del territorio;

- la tematica del recupero, riqualificazione e valorizzazione delle vallate genovesi appare fondamentale per imporre una svolta allo stato di abbandono e di degrado del territorio dell'entroterra genovese;

- le tematiche delle criticità geologiche e idrogeologiche, a causa degli eventi alluvionali, la predisposizione al dissesto del territorio, le modificazioni antropiche e climatiche, le aree produttive abbandonate e non risistemate, hanno raggiunto un rilievo di primo piano;

- per contrastare questo stato di degrado, occorre prontamente organizzare una serie di azioni che consentano il recupero, la riqualificazione e la valorizzazione del territorio collinare e montano genovese mediante interventi per la stabilizzazione e messa in sicurezza del territorio, il riordino del verde, il recupero dei sentieri e la realizzazione di nuove aree di sosta attrezzate o di svago;

- in collaborazione con i Municipi sono state individuate alcune aree di civica proprietà adatte alla realizzazione di parchi tecnologici, con allestimenti dedicati ad interventi mirati alla stabilizzazione dei versanti, con recupero di aree, alla regimazione delle acque, ma anche alla riqualificazione di aree sensibili attualmente in degrado che potrebbero essere recuperate sia come aree verdi aperte al pubblico sia come zone su cui veicolare il turismo.

Visto che:

- la Direzione Geotecnica ed Idrogeologia, Espropri, Vallate ha redatto un progetto di fattibilità tecnico economica mirato alla realizzazione di Parchi Geotecnici didattici aperti al pubblico su aree verdi di civica proprietà per il recupero e la valorizzazione del territorio;

- il Comune di Genova è interessato all'avvio di una collaborazione con la Fondazione Istituto Italiano di Tecnologia (IIT), in particolare, potrà includere le seguenti attività:

  a) l'accesso di personale di ciascuna Parte presso le strutture dell'altra;
  b) l'organizzazione di seminari, workshop o conferenze;
  c) la partecipazione a bandi per il finanziamento di interventi volti a valorizzare il territorio e lo sviluppo locale;

- la Direzione Idrogeologia e Geotecnica, Espropri, Vallate del Comune di Genova da alcuni anni provvede alla redazione di progetti per la messa in sicurezza idrogeologica e per la valorizza-

zione del territorio, seguendo criteri di sistemazione compatibili con l'ambiente e volti a recuperare e riqualificare le vallate;

Considerato:

- pertanto, di procedere, alla presa di atto del protocollo di intesa per la promozione di una collaborazione su tematiche geotecniche tra la Fondazione Istituto Italiano di Tecnologia e il Comune di Genova;

- che il protocollo d'intesa proposto, Prot. NP n. 1597 del 07/07/2023, allegato quale parte integrante al presente provvedimento, non comporta costi per la Pubblica Amministrazione;

- l'istruttoria del presente atto è stata svolta dal Dott. Geol. Giorgio Grassano, responsabile del procedimento, che attesta la regolarità e correttezza dell'azione amministrativa per quanto di competenza, ai sensi dell'art. 147 -*bis* del D. Lgs. 267/2000 e che provvederà a tutti gli atti necessari all'esecuzione del presente provvedimento, fatta salva esecuzione di ulteriori adempimenti posti a carico di altri soggetti;

- con la sottoscrizione del presente atto, il dirigente attesta altresì la regolarità e la correttezza dell'azione amministrativa, assieme al responsabile del procedimento, ai sensi dell'art. 147 bis del D. Lgs. n. 267/2000

DETERMINA

per i motivi di cui in premessa:

- di prendere atto del protocollo d'intesa, allegato quale parte integrante al presente testo, tra la Fondazione Istituto Italiano di Tecnologia e il Comune di Genova ;

- che è stata regolarmente accertata l'insussistenza di situazioni di conflitto di interessi, in attuazione dell'art. 6 -*bis* della L.241/1990;

- la presente determinazione dirigenziale non comporta alcuna assunzione di spesa o introito a carico del Bilancio comunale, né alcun riscontro contabile, né attestazione di copertura finanziaria;

- il presente provvedimento è regolare sotto il profilo tecnico, amministrativo e contabile ai sensi dell'art. 147 bis – comma 1 – del D. Lgs. 267/2000 (TUEL).

Il Direttore
Dott. Geol. Giorgio Grassano

Protocollo d'Intesa

TRA

Fondazione Istituto Italiano di Tecnologia, codice fiscale 97329350587, con sede legale in Genova, Via Morego n. 30, (di seguito, "IIT"), nella persona del suo Direttore Scientifico, Prof. Giorgio Metta, debitamente autorizzato alla firma del presente atto,

da una parte

E

Comune di Genova, codice fiscale 0856930102, con sede legale in Genova, Via Garibaldi, 9 (di seguito, "Comune"), rappresentato dal Sindaco, Dott. Marco Bucci, autorizzato alla firma del presente atto con deliberazione D.G.C. 2019/53 del 28.02.2019;

dall'altra

Nel prosieguo singolarmente e/o congiuntamente anche "la Parte" e/o "le Parti"

PREMESSO CHE

(a) IIT è una Fondazione senza scopo di lucro il cui principale obiettivo è promuovere l'eccellenza nella ricerca di base e applicata. Il Programma Scientifico di IIT è contraddistinto da una marcata multidisciplinarietà, con competenze in 4 ambiti principali di ricerca: Robotica, Nanomateriali, Tecnologie per le Scienze della Vita e Scienze Computazionali;
(b) Il Comune, per il tramite della sua Direzione Idrogeologia e Geotecnica, Espropri e Vallate, è attivo nel campo del riassetto idrogeologico e della riqualificazione ambientale del territorio collinare, sviluppando studi e progetti volti alla salvaguardia e prevenzione dei rischi idrogeologico - ambientali anche attraverso la valorizzazione degli aspetti geologici, paesaggistico-culturali e storici del territorio e realizzando i relativi lavori tramite specifici appalti.
(c) IIT e il Comune sono interessati ad incoraggiare una collaborazione secondo i termini e alle condizioni di seguito concordati.

Tutto ciò premesso, che costituisce parte integrante e sostanziale del presente atto (di seguito, "Protocollo d'Intesa"), le Parti stabiliscono quanto segue:

Articolo 1 – **OGGETTO**

1.1 Con il Protocollo d'Intesa le Parti intendono promuovere una collaborazione su **tematiche geotecniche**. La collaborazione, in particolare, potrà includere le seguenti attività:

- l'accesso di personale di ciascuna Parte presso le strutture dell'altra;
- l'organizzazione di seminari, workshop o conferenze;
- la partecipazione a bandi per il finanziamento di interventi volti a valorizzare il territorio e lo sviluppo locale;
- l'esecuzione di programmi congiunti di ricerca e sviluppo riguardanti a titolo esemplificativo e non esaustivo: la salvaguardia e prevenzione dei rischi idrogeologico – ambientali, la realizzazione di parchi geotecnici e il monitoraggio del territorio collinare.

1.2 Ove necessario o opportuno le modalità e i dettagli delle diverse attività di collaborazione saranno oggetto di appositi accordi scritti, che le Parti definiranno in buona fede sulla base delle specifiche esigenze.

Articolo 2 – **RISERVATEZZA**

2.1 Le Parti prendono atto che, nell'ambito del Protocollo d'Intesa e al fine della realizzazione delle attività che ne costituiscono il suo oggetto, ciascuna Parte potrà avere accesso o venire a conoscenza di informazioni, dati o conoscenze dell'altra Parte o comunque in suo legittimo possesso, di carattere tecnico, scientifico, commerciale, o di qualunque altra natura, di carattere riservato e segreto ("Informazioni Confidenziali"). Pertanto, ciascuna Parte si impegna fin da ora a:
(i) utilizzare le Informazioni Confidenziali nella misura e con i mezzi strettamente necessari allo svolgimento delle attività oggetto del Protocollo d'Intesa, e con modalità che non ne compromettano in alcun modo il carattere della riservatezza;
(ii) non divulgare o rendere in alcun modo accessibili a qualsiasi terza parte le Informazioni Confidenziali, né in tutto né in parte, direttamente o indirettamente, senza aver prima ottenuto un'autorizzazione scritta della Parte divulgante;
(ii) non utilizzare le Informazioni Confidenziali, né in tutto né in parte, direttamente o indirettamente, per fini diversi da quanto previsto dal Protocollo d'Intesa;
(iii) mettere in atto tutte le misure adeguate a garantire e mantenere la massima riservatezza delle Informazioni Confidenziali, nonché a impiegare la diligenza necessaria a prevenire usi non autorizzati, o divulgazioni interne o esterne indebite; e
(iv) non copiare, duplicare, riprodurre, memorizzare o registrare, con ogni e qualsiasi mezzo a tali fini idoneo, in tutto o in parte, direttamente o indirettamente, file, atti, documenti, disegni, schemi, e ogni altro materiale contenente una o più Informazioni Confidenziali, salvo consenso espresso dalla Parte che ne abbia diritto;
(v) limitare internamente l'accesso alle Informazioni Confidenziali a quei dipendenti, collaboratori o altro personale che, per competenze, funzioni o compiti specifici, si trovino nella necessità di conoscerle ed utilizzarle; tale divulgazione potrà in ogni caso avvenire soltanto a condizione che tali soggetti sottoscrivano un accordo di confidenzialità di contenuto analogo o comunque di portata non minore di quello del Protocollo d'Intesa.
2.2 La natura riservata delle Informazioni Confidenziali dovrà essere evidenziata mediante indicazione della dicitura "riservato", "confidenziale" o con simile legenda; le informazioni divulgate verbalmente o visivamente dovranno essere identificate dalla parte divulgante come "Informazioni Confidenziali" al momento della loro divulgazione, e la relativa confidenzialità dovrà essere tempestivamente confermata dalla parte divulgante con una comunicazione scritta da trasmettersi alla parte ricevente entro 15 (quindici) giorni dall'avvenuta divulgazione.
Resta inteso che, l'assenza di tali esplicite indicazioni circa la riservatezza, in ogni caso, non precluderà la qualificazione di un'informazione come "Informazione Confidenziale" se il divulgante è in grado di provare la sua natura confidenziale, o se il ricevente conosceva o avrebbe dovuto conoscere la sua natura confidenziale, proprietaria o segreta per il divulgante.

2.3 Resta inteso tra le Parti che in nessun caso possono essere considerate Informazioni Confidenziali quelle che siano già di pubblico dominio al momento della loro divulgazione alla Parte ricevente, o che lo diventino successivamente per cause indipendenti dalla volontà e dal contegno della Parte ricevente.

2.4 Ciascuna Parte garantisce che il proprio personale, dipendente, consulente e/o collaboratore, destinato allo svolgimento delle attività oggetto del Protocollo d'Intesa manterrà nei confronti di qualsiasi terzo non autorizzato la riservatezza per quanto attiene alle Informazioni Confidenziali di cui dovesse venire a conoscenza, nonché per quanto attiene ai risultati conseguiti. A tal fine, ciascuna Parte si impegna sin d'ora a tenere indenne e manlevare l'altra Parte per ogni danno o pregiudizio quest'ultima abbia a subire in connessione e/o in dipendenza con eventuali violazioni delle disposizioni del presente articolo, posti in essere dall'altra Parte e/o dai propri dipendenti, consulenti e/o collaboratori, a meno che la Parte inadempiente non provi che tale violazione si sia verificata nonostante l'uso della migliore diligenza in rapporto alle circostanze.
2.5 Gli obblighi di cui al presente articolo resteranno validi per la durata del Protocollo d'Intesa e per un periodo di 5 (cinque) anni successivo alla data di scadenza o cessazione, per qualsivoglia motivo, dello stesso.

Articolo 3 – **PROPRIETA' INTELLETTUALE**

3.1 Ciascuna Parte è e rimane titolare delle conoscenze, del know-how e delle informazioni di cui era già titolare prima della sottoscrizione del Protocollo d'Intesa, nonché di tutti i diritti di proprietà intellettuale ad esse relative (di seguito "Background"), e che ha reso disponibili all'altra Parte in occasione delle attività oggetto del Protocollo d'intesa. Il Background costituisce Informazione Confidenziale della Parte che lo mette a disposizione dell'altra al fine dell'esecuzione delle attività congiunte, e dovrà, pertanto, essere trattato in conformità con quanto disposto al precedente articolo 2.
3.2 Resta espressamente inteso che, con il Protocollo d'Intesa, le Parti non concedono né trasferiscono alcun diritto, neanche implicito, a favore dell'altra Parte, in relazione al proprio Background.

Articolo 4 – **SICUREZZA DELLE INFORMAZIONI**

Le Parti concordano sin d'ora che qualunque informazione in formato digitale trattata all'interno del Protocollo d'Intesa o degli ulteriori accordi che ne costituiscono attuazione sarà gestita e formalizzata secondo le modalità previste dall'Allegato 1 "Misure di sicurezza tecnico-organizzative ICT", qui fornito in forma di facsimile.

Articolo 5 – **TRATTAMENTO DEI DATI PERSONALI**

5.1 Le Parti dichiarano espressamente di essere informate e di acconsentire che i dati personali forniti nel corso dell'esecuzione del Protocollo d'Intesa saranno trattati esclusivamente per le finalità del Protocollo d'Intesa medesimo e, in ogni caso, nel rispetto di tutte le disposizioni dettate dal Regolamento UE 2016/679 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 dalla normativa applicabile in materia di protezione dei dati personali.

5.2 Le Parti concordano sin d'ora che il trattamento dei dati personali avverrà nel rispetto delle misure di sicurezza organizzative di cui all'Allegato 2 "Misure di sicurezza organizzative relative ai dati personali", qui fornito in forma di facsimile.

5.3 Le Parti si impegnano altresì ad adempiere, ove necessario, agli obblighi di informativa e di consenso derivanti dal predetto Regolamento nei confronti delle persone fisiche coinvolte nelle attività oggetto del Protocollo d'Intesa.

ART. 6 – **GESTIONE DEI DATA BREACH**

6.1 Tenendo conto della natura del trattamento e delle informazioni a disposizione, ciascuna delle Parti si impegna ad informare tempestivamente l'altra Parte, a mezzo PEC, agli indirizzi di ciascuna indicati all'art 13 (Comunicazioni Amministrative), inserendo in cc l'indirizzo email gdpr@iit.it, ogniqualvolta sia ragionevolmente certa che la violazione che si è verificata nell'ambito del Protocollo d'Intesa e/o degli accordi scritti di cui all'articolo 1.2 comporti la compromissione di dati personali ("data breach"), fermo restando, da parte di ciascun Titolare autonomo del trattamento, il rispetto degli articoli 33 e 34 del GDPR. Ai sensi dell'articolo 82.2 del GDPR, ciascuna delle Parti è tenuta a rispondere per il danno cagionato dal suo trattamento che violi il Regolamento.

Articolo 7 – **DURATA**

7.1 Il Protocollo d'Intesa avrà durata pari a cinque (5) anni a decorrere dalla data della sua ultima sottoscrizione e potrà essere rinnovato soltanto previo espresso accordo scritto tra le Parti, dovendo intendersi escluso il tacito rinnovo.

Articolo 8 **– RECESSO**

Ciascuna Parte si riserva il diritto di recedere dal presente Protocollo d'Intesa, in ogni momento ed a suo insindacabile giudizio, mediante preavviso di 30 (trenta) giorni da comunicare all'altra Parte mediante lettera raccomandata A/R o tramite pec agli indirizzi indicati nel successivo art. 13 (Comunicazioni amministrative).

Articolo 9 – **USO DEI SEGNI DISTINTIVI**

9.1 Il contenuto del Protocollo d'Intesa non conferisce alle Parti alcun diritto di usare, per scopi pubblicitari o per qualunque altra attività promozionale, alcun nome, marchio, o altra designazione dell'altra Parte, incluse le abbreviazioni ("Segni Distintivi"). Eventuali eccezioni potranno essere pattuite dalle Parti tramite separato accordo scritto. Sono in ogni caso fatti salvi gli usi liberi di legge, ex art. 21 del D. Lgs. n. 30/2005 "Codice della Proprietà Industriale", della sola denominazione in funzione descrittiva, purché resa in forma veritiera.

9.2 Fermo restando quanto sopra, le Parti si concedono reciprocamente l'autorizzazione ad utilizzare i rispettivi Segni Distintivi al solo ed esclusivo fine di dare risalto all'attività collaborativa di cui al Protocollo d'Intesa, limitatamente alla sua durata. Le Parti, tramite i rispettivi uffici a ciò preposti, definiranno le modalità operative d'utilizzo dei Segni Distintivi. Per quanto concerne IIT, il Comune dovrà fare riferimento a roo@iit.it e, per quanto riguarda il Comune, IIT dovrà fare riferimento al Dott. Giorgio Grassano, Direttore della Direzione Idrogeologia e Geotecnica, Espropri e Vallate del Comune di Genova.

Articolo 10 **– CONTROVERSIE E FORO COMPETENTE**

10.1 Laddove sorgessero controversie tra le Parti in merito all'applicazione, interpretazione, o esecuzione del Protocollo d'Intesa le Parti si impegnano ad addivenire ad un amichevole componimento delle stesse.

10.2 In caso di mancato raggiungimento di un accordo a seguito del tentativo di composizione amichevole di cui al punto precedente, le Parti eleggono il Foro di Genova quale foro competente ed esclusivo.

Articolo 11 **– REGISTRAZIONE**

Il Protocollo d'Intesa sarà registrato in solo caso d'uso a tassa fissa ai sensi degli Articoli 5 e 39 del D.P.R. 131/86. Tutte le spese relative all'eventuale registrazione rimarranno ad esclusivo onere e carico della Parte richiedente.

Articolo 12 **– CESSIONE**

Nessuna delle Parti potrà cedere a terzi, in tutto o in parte, il Protocollo d'Intesa o i diritti e le obbligazioni nascenti dallo stesso in capo a ciascuna Parte, se non previo espresso consenso scritto dell'altra Parte.

Articolo 13 – **COMUNICAZIONI AMMINISTRATIVE**

Ogni comunicazione tra le Parti ai sensi del Protocollo d'Intesa dovrà essere effettuata per iscritto ai seguenti indirizzi, o a quelli successivamente indicati con le stesse modalità da una Parte all'altra:

Se a IIT:

Fondazione Istituto Italiano di Tecnologia - Via Morego, 30 – 16163 Genova – Direzione per l'Organizzazione della Ricerca, all'attenzione del Prof. Giorgio Metta - Direttore Scientifico o all'indirizzo pec: roo@pec.iit.it

Se al Comune:

Dott. Giorgio Grassano, Direttore Direzione Idrogeologia e Geotecnica, Via di Francia 1, 16149 Genova

Dott. Alessio Bevilacqua, Consigliere Delegato alle Vallate, Via Garibaldi 9, 16124 Genova

Articolo 14 – **ADEMPIMENTI EX LEGE 231/2001**

Il Comune dichiara di essere a conoscenza della normativa vigente in materia di responsabilità amministrativa degli enti e, in particolare, del Decreto Legislativo 8 giugno 2001, n. 231 e di aver preso atto del Codice di Comportamento e di Condotta Scientifica nonché del Modello di Organizzazione, Gestione e Controllo adottati da IIT ai sensi della predetta normativa (disponibili al seguente link: https://www.iit.it/it/web/guest/trasparenza).

Articolo 15 – **CONFLITTO DI INTERESSI**

Le Parti dichiarano di aver adottato tutte le misure atte a prevenire e contrastare il conflitto di interessi e di averle recepite nella propria normativa e documentazione interna e pertanto si impegnano ad applicarle qualora emerga che i soggetti coinvolti a qualunque titolo nell'esecuzione del Protocollo d'Intesa denuncino l'esistenza, anche apparente, di tale conflitto.

Letto, confermato e sottoscritto digitalmente

Fondazione Istituto Italiano di Tecnologia	**Comune di Genova**
Prof. Giorgio Metta (Direttore Scientifico)	Dott. Pietro Piciocchi (Vicesindaco, Assessore ai Lavori Pubblici e Bilancio)

Allegato 1: Misure di sicurezza tecnico-organizzative ICT - Facsimile
Allegato 2: Misure di sicurezza organizzative relative ai dati personali – Facsimile

ALLEGATO 1
MISURE DI SICUREZZA TECNICO-ORGANIZZATIVE ICT - FACSIMILE

1. MISURE DI SICUREZZA

Nelle tabelle di seguito riportate sono indicate le misure di sicurezza, divise in "organizzative" e "tecniche", la cui implementazione deve essere garantita a protezione delle informazioni in formato digitale trattate all'interno del Protocollo d'Intesa o degli ulteriori accordi che ne costituiscono attuazione da ciascuna Parte coinvolta per mezzo di un suo referente tecnico indicato nei paragrafi sottostanti.

Ciascuna Parte dovrà essere in grado, se richiesto dall'altra Parte, di fornire evidenza della conformità ai controlli selezionati. Nel caso in cui una Parte non sia in grado di soddisfare in tutto o in parte un obiettivo di controllo, è tenuta a segnalarlo all'altra Parte, fornendo le necessarie motivazioni e informazioni ed evidenza dei controlli compensativi rilevanti all'interno del presente allegato.

In caso di ricorso a fornitori (sub-responsabili) per la gestione dei servizi informatici e di sicurezza l'applicazione delle misure sotto descritte dovrà essere traferita contrattualmente ai fornitori stessi. Ciascuna Parte si impegna inoltre a tener traccia dei fornitori coinvolti in un registro apposito, che può essere richiesto dall'altra Parte per verifica e controllo.

Ogni qualvolta si verifichi un incidente di sicurezza che coinvolga le Informazioni trattate, questo dovrà essere comunicato tempestivamente ai referenti individuati nei paragrafi sottostanti, e comunque entro le 24 ore successive all'evento nel caso l'incidente possa comportare una violazione di dati personali.

1.1. Misure di sicurezza organizzative

Item #	**Categoria**	**Controllo**	**Compliance status IIT** (S/N/n.a.)	**Compliance status Comune** (S/N/n.a.)	**Note giustificative** (se non applicabile, non implementato o parzialmente implementato, darne motivazione indicando i controlli compensativi applicati in sostituzione)
1	Policy di Sicurezza delle Informazioni	L'organizzazione deve documentare la propria politica per quanto riguarda l'elaborazione dei dati come parte della politica di sicurezza informatica. La politica di sicurezza deve essere riesaminata e riveduta, se necessario, su base annua. La politica di sicurezza deve almeno riferirsi a: ruoli e responsabilità del personale, le misure tecniche e organizzative di base adottate per la			

		sicurezza dei dati, i responsabili dei dati o altre terze parti coinvolte nel trattamento di dati. La politica deve essere approvata dalla direzione e comunicata a tutti i dipendenti e alle parti esterne pertinenti.			
2	Ruoli e Responsabilità per la Sicurezza delle Informazioni	Deve essere identificato un responsabile della sicurezza delle informazioni, a cui devono essere comunicati i relativi compiti e responsabilità. Deve essere effettuata una chiara nomina dei responsabili aventi specifici compiti di sicurezza. Durante le re-organizzazioni interne o le cessazioni dei rapporti di lavoro o la modifica anche temporanea della mansione, la revoca dei diritti e delle responsabilità e le rispettive autorizzazioni devono essere definite chiaramente.			
3	Sicurezza delle Risorse Umane, Consapevolezza e Formazione	Prima iniziare il rapporto di lavoro ai dipendenti deve essere chiesto di prendere visione del documento o della politica di sicurezza dell'organizzazione e di firmare i rispettivi accordi di riservatezza e di non divulgazione. L'organizzazione deve avere programmi di formazione e sensibilizzazione strutturati e regolari per il personale, compresi programmi specifici relativi alla protezione dei dati. Il piano di formazione deve essere preparato ed eseguito su base annua, o con altra periodicità ritenuta adeguata.			
4	Policy di gestione degli asset	L'organizzazione deve documentare la propria politica per quanto riguarda l'utilizzo delle risorse informatiche aziendali.			
5	Policy di gestione dei dispositivi portatili	Devono essere definite e documentate delle policy e procedure per la gestione e l'uso corretto dei dispositivi mobili, comprendenti l'utilizzo o meno di dispositivi personali e l'utilizzo di dispositivi aziendali per usi personali, e la definizione di ruoli specifici e responsabilità per quanto riguarda la gestione dei dispositivi mobili.			

6	Policy per il Controllo degli Accessi	Autorizzazioni specifiche per il controllo dell'accesso ai dati devono essere assegnate a ciascun ruolo in seguito alla necessità del rispetto del principio del “need to know”. I criteri di controllo accesso devono essere dettagliati e documentati. L'organizzazione deve determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per ruoli utente specifici verso i processi e le procedure relative ai dati trattati. Il principio della “Segregation of Duty” (ad es. richiesta di accesso, autorizzazione di accesso, amministrazione dell'accesso) deve essere chiaramente definito e documentato.			
7	Procedure operative e responsabilità	Deve essere definita e aggiornata regolarmente una politica per la gestione dei cambiamenti che deve includere: un processo per l'introduzione di modifiche, i ruoli/utenti che hanno diritti di cambiamento, le timeline per l'introduzione di modifiche, la tracciatura delle modifiche e il loro monitoraggio. Deve essere svolto un controllo periodico di questo processo.			
8	Gestione degli incidenti relativi alla sicurezza delle informazioni	Deve essere definito e documentato un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti. Il piano deve assicurare che le violazioni dei dati personali siano immediatamente segnalate al Titolare entro gli accordi contrattualizzati.			
9	Continuità della sicurezza delle informazioni	Deve essere dettagliato e documentato un Piano di Continuità operativa che preveda azioni ben definite e l'assegnazione dei ruoli. Nel piano deve essere definito un livello di qualità del servizio per i processi aziendali che forniscono servizi critici per la protezione dei dati. Deve essere identificato e nominato personale specifico con la responsabilità necessaria, l'autorità e la competenza per gestire la continuità aziendale in caso di incidente/violazione dei dati personali. Una struttura alternativa deve essere considerata, a seconda dell'organizzazione e del tempo di inattività accettabile del sistema IT.			

10	Conformità alla sicurezza delle informazioni	L'organizzazione deve svolgere con cadenza almeno annuale una verifica (o audit interno) delle proprie misure tecniche e organizzative per l'implementazione di eventuali azioni correttive.			

1.2. Misure di sicurezza tecniche

ID	**Categoria**	**Controllo**	**Compliance status IIT** (S/N/n.a.)	**Compliance status Parte XXX** (S/N/n.a.)	**Note giustificative** (se non applicabile, non implementato o parzialmente implementato, darne motivazione indicando i controlli compensativi applicati in sostituzione)
1	Gestione degli accessi e delle credenziali	Devono essere applicate misure di sicurezza agli accessi logici, come password robuste (o equivalente codice di protezione per dispositivi mobili) e modifica periodica delle stesse. Deve essere effettuata una revisione periodica dei permessi di accesso, ad esempio in caso di cessazione del rapporto con la Società o di cambiamenti interni all'organizzazione.			
2	Firewall	Deve essere attivato un firewall di rete, che permetta solo il traffico e i servizi necessari.			
3	Inventario	Gli asset gestiti (incluse le applicazioni) devono essere registrati in un inventario con le loro informazioni di rilievo, e aggiornati con periodicità non maggiore a 6 mesi.			
4	Patching	Devono essere usate versioni supportate di applicazioni e sistemi operativi. Le patch di sicurezza classificate come "critiche" e "gravi" devono essere applicate entro 20 giorni dal rilascio, tutte le altre entro 90 giorni.			
5	Protezione da Malware	Deve essere installato e tenuto aggiornato un agente antivirus/anti-malware.			
6	Gestione delle vulnerabilità	Deve essere effettuata una scansione di vulnerabilità almeno ogni 3 mesi e le vulnerabilità ad alto rischio riscontrate devono essere risolte entro 10 giorni.			

7	Backup	Deve essere effettuato un backup almeno settimanale di dati e configurazioni. I dati di backup devono essere cifrati in transito e quando salvati su supporti esterni, e testati regolarmente per assicurarsi che possano essere usati in caso di necessità.			
8	Sicurezza delle Comunicazioni	Le informazioni trasferite su canali applicativi devono essere cifrate nel trasporto, ad esempi usando protocolli sicuri (TLS, https, ssh) o canali cifrati (VPN).			
9	Cancellazione sicura	Quando non più necessari, i dati devono essere rimossi in maniera permanente con tecniche di cancellazione sicura. Per i device remoti, ciò deve poter essere controllato centralmente.			
10	Cifratura	Deve essere prevista la cifratura delle unità d'archiviazione, quali dischi rigidi (in particolare dei laptop), dischi e chiavette USB, DVD, backup tapes, ecc. Per i file, i record o i campi più critici devono essere considerate soluzioni di cifratura, adottandole ove possibile.			
11	Gestione dei log	I log, inclusi quelli degli Amministratori di Sistema, devono essere inviati ad un sistema di raccolta centrale, che ne prevenga l'alterazione. Per le applicazioni cloud, tali log devono essere resi disponibili ed esportati su richiesta entro 5 giorni.			
12	Sicurezza fisica	Le server room e i datacenter devono essere ad accesso controllato e provviste di misure di sicurezza fisica (antincendio, antiallagamento, controllo della temperatura, continuità elettrica).			
13	Revisione degli aspetti di Sicurezza, di Privacy e Legali	Deve essere eseguita una verifica degli aspetti di security, privacy e legali ed implementate le raccomandazioni conseguenti prima dell'utilizzo in produzione di applicazioni che trattano dati personali.			
14	Sviluppo di software sicuro	Lo sviluppo sicuro deve avvenire secondo i principi di privacy-by design e security-by-design. In particolare, gli ambienti di test devono essere separati dagli ambienti di produzione e non devono utilizzare dati reali.			

15	Autenticazione forte	Deve essere implementato un sistema di autenticazione a 2 fattori per accessi degli amministratori di sistema e per tutti gli accessi a sistemi utilizzati per il trattamento di dati genetici o qualificati come "a maggior tutela".			

1.3. Referente tecnico di XXX verso IIT

Per informazioni sulle checklist dei controlli di sicurezza organizzativi e tecnici, IIT può fare riferimento a:

Nome, Cognome .....
Indirizzo e-mail .....
Contatto telefonico .....

1.4. Referente tecnico di IIT verso XXX

Per informazioni sulle checklist dei controlli di sicurezza organizzativi e tecnici, XXX può fare riferimento a:

Contatto primario:
Nome, Cognome .....
Indirizzo e-mail .....
Contatto telefonico .....

Contatto secondario:
Stefano Bencetti (ICT Director)
stefano.bencetti@iit.it
[redacted]

ALLEGATO 2

MISURE DI SICUREZZA ORGANIZZATIVE RELATIVE AI DATI PERSONALI - FACSIMILE

2. MISURE DI SICUREZZA ORGANIZZATIVE

Nella tabella di seguito riportata sono indicate le misure di sicurezza organizzative relative ai dati personali previste da IIT ai sensi del Regolamento Generale sulla protezione dei dati personali n. 679/2016 e s.m.i. (di seguito "GDPR"), per cui si richiede al Comune la dimostrazione della conformità attraverso la compilazione della colonna "Compliance Status Partner".

Nel caso in cui il Comune non sia in grado di soddisfare in tutto o in parte i requisiti richiesti, è tenuto a specificarne la motivazione nella colonna "Note giustificative".

2.1. Misure di sicurezza organizzative

Item #	**Categoria**	**Controllo**	**Compliance status IIT** (S/N/n.a.)	**Compliance status Comune** (S/N/n.a.)	**Note giustificative** (se non applicabile, non implementato o parzialmente implementato, darne motivazione indicando i controlli compensativi applicati in sostituzione)
1	Analisi dei rischi	È stata effettuata l'analisi dei rischi e sono stati definiti ed implementati gli action plan per l'adeguamento delle misure di sicurezza organizzative (laddove necessario). L'analisi dei rischi viene costantemente aggiornata.			
2	Attribuzione di funzioni e compiti a soggetti autorizzati	Il personale interno che tratta dati personali è designato con apposito atto di nomina.			
3	Istruzioni al personale interno autorizzato al trattamento dei dati personali	Comunicazione di apposite istruzioni scritte al personale interno autorizzato al trattamento dei dati personali.			

4	Canale dedicato per la notifica delle violazioni di Dati Personali (se applicabile)	È disponibile un apposito canale per la comunicazione delle eventuali violazioni degli obblighi in tema di trattamento di Dati Personali.			
5	Designazione del Responsabile della Protezione dei Dati (se applicabile)	È designato un Responsabile della Protezione dei Dati a cui è affidato il compito di valutare ed organizzare la gestione del trattamento dei dati personali.			
6	Pseudonimizzazione dei dati personali (laddove applicabile):	Applicazione di misure di de-identificazione dei dati personali, in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive. Le informazioni aggiuntive sono conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.			

2.2. Referente GDPR di XXX verso IIT

Per informazioni sulla checklist dei controlli di sicurezza organizzativi, IIT può fare riferimento a:

Nome, Cognome .....
Indirizzo e-mail .....
Contatto telefonico .....

2.3. Referente GDPR di IIT verso XXX

Per informazioni sulla checklist dei controlli di sicurezza organizzativi, XXX può fare riferimento a:

GDPR Team
gdpr@iit.it
[redacted]