PA-POMPEI|30/05/2024|CONVENZIONI ITALIA 23

ACCORDO N. 4
PER LO SVOLGIMENTO DEL PROGRAMMA DI RICERCA
"Caratterizzazione e conservazione delle pitture parietali pompeiane"

in attuazione della Convenzione Quadro stipulata in data 12/04/2023 (Prot. IIT n.2683/23, conv. PAP n.18 13/04/2023) fra il Parco Archeologico di Pompei (di seguito "PAP") e la FONDAZIONE ISTITUTO ITALIANO DI TECNOLOGIA (di seguito "IIT")

di seguito denominate anche, singolarmente e/o congiuntamente, "la Parte" e/o "le Parti"

1. Titolo del Programma di Ricerca oggetto dell'Accordo
Caratterizzazione e conservazione delle pitture parietali pompeiane: il Programma di Ricerca è volto allo studio e alla conservazione delle pitture murali pompeiane.

2. Descrizione dettagliata del Programma di Ricerca
Il Programma di Ricerca è relativo a interventi di caratterizzazione di pitture murali pompeiane per casi specifici indicato da PAP al fine di svolgere interventi conservativi ritenuti d'interesse dai tecnici del Parco stesso.
IIT utilizzerà un approccio multi-analitico e trans-disciplinare che prende in considerazione sia lo strato pittorico che i tectoria, i.e. gli strati preparatori di malta che ne determinano l'adesione al supporto murario. Tale approccio prevede l'utilizzo di tecniche non invasive e non distruttive quali le analisi iperspettrali (HSI) in due diversi range operativi, VIS-NIR (400-1000 nm) e SWIR (900-1700 nm), e il ricorso a tecniche invasive ove necessario, concordate con il Parco Archeologico di Pompei. In supporto all'analisi non-invasiva, IIT potrà effettuare, di comune accordo con PAP e previa opportuna autorizzazione, la caratterizzazione localizzata degli affreschi attraverso il prelievo di micro-campioni. I campioni prelevati vengono in questi casi analizzati seguendo la metodologia riportata nella Norma Europea UNI EN 17187 circa la Caratterizzazione delle malte utilizzate nel Patrimonio Culturale. La caratterizzazione approfondita delle pitture murali e delle forme di degrado presenti potrà essere propedeutica alla selezione di opportuni consolidanti e protettivi da proporre ai restauratori di PAP per attuare interventi conservativi mirati.
Sulla base di tali considerazioni, si elencano le attività che saranno perseguite nel corso del programma congiunto di collaborazione:
- caratterizzazione di frammenti di affresco distaccati dalle pareti per supportare il loro ricollocamento in sede di origine, ove possibile;
- creazione in laboratorio di repliche (mock-up) che riproducano il caso reale, per poter effettuare tutti i necessari test preliminari;
- identificazione di eventuali consolidanti e protettivi tra i prodotti sviluppati da IIT, ritenuti idonei da ambi le istituzioni e la loro applicazione al caso reale.
I test effettuati su mock-ups consentiranno inoltre di comprendere meglio quali siano le performance dei prodotti sviluppati anche in ambienti differenti rispetto al caso di studio considerato di volta in volta, estendendo l'ambito della ricerca ad altri contesti d'interesse. A valle delle prove in laboratorio si potrà valutare l'opportunità di eseguire test sul campo, con interventi ad hoc sulle pitture murali reali.

3. Team di Ricerca

Per l'esecuzione del Programma di Ricerca ciascuna Parte individua un Responsabile Scientifico e il personale che prenderà parte alle attività di ricerca. I Responsabili avranno il compito di predisporre e definire nel dettaglio il Programma di Ricerca, nonché di valutare periodicamente e concordare eventuali aggiornamenti al piano di attività.

Per PAP:

- **Responsabile Scientifico:** *Alessandra Zambrano, funzionario ingegnere*
- **Personale (dipendente e collaboratori del Parco Archeologico di Pompei) coinvolto:** *Il gruppo di lavoro sarà definito con atto amministrativo del PAP*

Per IIT:

- **Responsabile Scientifico:** *Arianna Traviglia, researcher, coordinatrice del centro CCHT.*
- **Personale (dipendente e collaboratori di IIT, nonché eventuale personale affiliato a IIT) coinvolto:**
    - *Raffaella Lamuraglia, PhD Student;*
    - *Agnese Babini, Post Doc;*
    - *Francesco Abate, PhD Student.*

Ciascuna Parte ha facoltà di sostituire il Responsabile Scientifico e/o il personale coinvolto di propria indicazione mediante comunicazione scritta da inviare all'altra Parte con indicazione del nominativo del nuovo membro e di quello che si intende sostituire.

4. Durata del Programma di Ricerca e diagramma temporale

Il programma avrà una durata di 3 anni.

Nel primo anno si effettueranno le caratterizzazioni non invasive, si valuteranno i punti di prelievo più rappresentativi sulla base delle indicazioni dei tecnici del Parco Archeologico di Pompei e si eseguiranno test in laboratorio circa le performance dei prodotti sviluppati miratamente per il restauro degli affreschi. Entro la fine del secondo anno, i prodotti selezionati saranno applicati sui casi reali e le performance saranno periodicamente monitorate *in situ*. Ulteriori test ed eventuali prove presso il parco saranno condotti nel terzo anno della ricerca.

5. Relazioni tecniche

Le Parti, con cadenza annuale, provvederanno congiuntamente e per iscritto a relazionare brevemente sullo stato di avanzamento del Programma di Ricerca. La relazione potrà consistere anche nella presentazione di un .ppt che verrà poi fornito alle controparti.

6.Laboratori/locali coinvolti nella collaborazione

Ad integrazione di quanto stabilito all'articolo 10 (Sicurezza e Ambiente) della Convenzione Quadro e ferma restando la responsabilità del datore di lavoro della Parte ospitante al rispetto della normativa vigente riguardante la conformità dei luoghi e delle attrezzature di lavoro di sua proprietà, le Parti si impegnano a:

- garantire la rispondenza dei propri locali, spazi e attrezzature, messi a disposizione per lo svolgimento delle attività previste dall'Accordo, con particolare riferimento alle disposizioni in materia di urbanistica, di salute e sicurezza sul lavoro, ambientale e di prevenzione incendi;

- garantire che le macchine, le attrezzature e le opere provvisionali ivi utilizzate e messe a disposizione dei lavoratori siano conformi alla normativa vigente e regolarmente soggette a verifica e manutenzione;
- garantire che i dispositivi di protezione individuale messi a disposizione dei lavoratori siano conformi ai requisiti previsti dalla normativa vigente e mantenuti in efficienza.

7. Impegni delle Parti

Ciascuna Parte, tenuto conto delle proprie disponibilità, sosterrà in autonomia i costi e le spese necessari per lo svolgimento delle attività di cui al Programma di Ricerca. In particolare, ciascuna Parte rimane esclusiva responsabile di: (i) la retribuzione del proprio personale coinvolto nel Programma di Ricerca, inclusi eventuali costi di trasferta, vitto ed alloggio; (ii) le spese connesse all'utilizzo dei propri laboratori, delle attrezzature e del materiale necessario allo svolgimento delle attività inerenti il Programma di Ricerca.

8. Sicurezza delle Informazioni e dei dati personali

Ad integrazione di quanto disposto all'art. 13 e art. 14 della Convenzione Quadro, rubricati "Sicurezza delle Informazioni" e "Trattamento dei dati personali" le Parti si impegnano ad adottare le misure indicate agli allegati 1 e 2 del presente programma di ricerca.

9. Recesso e Risoluzione

9.1 Ciascuna Parte si riserva il diritto di recedere dal presente Accordo 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.

9.2 Ciascuna Parte si riserva, altresì, il diritto di risolvere il presente Accordo in caso di inadempimento, da parte dell'altra Parte, di uno degli obblighi previsti dagli articoli 5 (Pubblicazioni), 6 (Obblighi di riservatezza), 7 (Gestione della proprietà intellettuale), 8 (trasferimento dei materiali), 9 (Garanzie), 10 (Sicurezza e ambiente), 13 (Sicurezza delle informazioni), 14 (Trattamento dei dati personali) e 15 (Gestione degli incidenti informatici e del Data Breach) della Convenzione Quadro, mediante lettera raccomandata A.R. o comunicazione a mezzo pec da notificare all'altra Parte con preavviso di 30 (trenta) giorni, salvo che la Parte inadempiente non provveda a sanare la propria situazione di inadempienza durante tale periodo di preavviso.

10. Rinvio

Resta inteso che, per quanto qui non espressamente previsto e/o richiamato, restano ferme le previsioni contenute nella Convenzione Quadro intervenuta tra le Parti e che, laddove non diversamente precisato, i termini utilizzati nel presente Accordo hanno lo stesso significato ad essi attribuito nella Convenzione Quadro.

Visto, approvato e sottoscritto digitalmente.

Parco Archeologico di Pompei
Dott. Gabriel Zuchtriegel
Direttore Generale

Fondazione Istituto Italiano di Tecnologia
Prof. Giorgio Metta
Direttore Scientifico

Firmato digitalmente da:

GABRIEL JOHANNES ZUCHTRIEGEL

POMPEII
PARCO ARCHEOLOGICO DI POMPEI

MINISTERO DELLA CULTURA

ISTITUTO ITALIANO DI TECNOLOGIA

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

ALLEGATO 1
MISURE DI SICUREZZA TECNICO-ORGANIZZATIVE ICT

1. MISURE DI SICUREZZA

Nel contesto della sicurezza delle informazioni è fondamentale comprendere che il grado di rischio associato ad un trattamento di dati può variare significativamente in base alla natura e alla sensibilità delle informazioni gestite. Deve quindi essere garantita l'adozione di misure di sicurezza adeguate a proteggere le 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 del Responsabile della Direzione ICT o del Responsabile della Sicurezza delle Informazioni (CISO), come indicato nei paragrafi sottostanti.

Le misure di sicurezza riportate nelle tabelle sottostanti, divise in "organizzative" e "tecniche", rappresentano quindi un insieme di linee guida di base minime, riportate a titolo non esaustivo, che dovrebbero essere implementate nei sistemi a perimetro degli accordi operativi che vengono a costituirsi fra le Parti. Pertanto, tali misure devono costituire il punto di partenza e, in caso di trattamenti dei dati considerati ad alto rischio, dovranno essere rivalutate e, se necessario, rafforzate al fine di garantire una protezione adeguata e la conformità alle normative vigenti.

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 una misura di sicurezza tecnica o non la ritenga applicabile dovrà fornire le necessarie motivazioni ed evidenze circa gli eventuali controlli compensativi adottati.

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 contatti individuati nel paragrafo sottostante.

1.1. Contatti dei Responsabili e dei referenti tecnici delle Parti

Responsabile ICT (CIO) e/o Responsabile Sicurezza delle Informazioni (CISO) di PAP

Nome, Cognome Vincenzo Calvanese

Indirizzo e-mail vincenzo.calvanese@cultura.gov.it
Contatto telefonico 081 8575225

Referente tecnico di PAP verso IIT

Come Referente dei controlli di sicurezza organizzativi e tecnici, IIT può fare riferimento a:

Nome, Cognome Raffaele Martinelli
Indirizzo e-mail raffaele.martinelli@cultura.gov.it
Contatto telefonico 081 8575302

Responsabile ICT di IIT

Stefano Bencetti (ICT Director)
stefano.bencetti@iit.it
+39 010 2896 505

Referente tecnico di IIT verso PAP

Come Referente dei controlli di sicurezza organizzativi e tecnici, PAP può fare riferimento a:

Matteo Brunettini (Responsabile Service Desk IIT)
ICT_Servicedesk@iit.it
+39 010 2896 555

1.2. Misure di sicurezza organizzative

Item #	Categoria	Controllo	Compliance IIT (S/N/n.a.)	Compliance PAP (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 di sicurezza delle informazioni. 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, ivi inclusa l'individuazione di un responsabile della sicurezza delle informazioni,	S	S	

		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	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.	**S**	**S**	
3	Policy di gestione degli asset	L'organizzazione deve documentare la propria politica per quanto riguarda l'utilizzo delle risorse informatiche aziendali, ivi inclusi i dispositivi mobili e quelli personali.	**S**	**S**	
4	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 documentare 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	**S**	**S**	

		of Duty" (ad es. richiesta di accesso, autorizzazione di accesso, amministrazione dell'accesso) deve essere chiaramente definito e documentato.			
5	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.	**S**	**S**	
6	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. Deve essere eseguita una verifica degli aspetti di security ed implementate le raccomandazioni conseguenti prima dell'utilizzo in produzione di applicazioni che trattano dati personali.	**S**	**S**	

1.3. Misure di sicurezza tecniche

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.

Firewall

Deve essere attivato un firewall di rete, che permetta solo il traffico e i servizi necessari.

Inventario
Gli asset gestiti (incluse le applicazioni) devono essere registrati in un inventario con le loro informazioni di rilievo, e mantenuti aggiornati.

Patching
Devono essere usate versioni supportate di applicazioni e sistemi operativi. Le patch di sicurezza classificate come "critiche" e "gravi" devono essere applicate con priorità e secondo un piano definito.

Protezione da Malware
Deve essere installato e tenuto aggiornato un agente antivirus/anti-malware.

Gestione delle vulnerabilità
Deve essere effettuata regolarmente una scansione di vulnerabilità e le vulnerabilità ad alto rischio riscontrate devono essere risolte con priorità secondo un piano definito.

Backup
Deve essere effettuato regolarmente un backup di dati e configurazioni. I dati di backup devono essere cifrati in transito e quando salvati su supporti esterni, e testati per assicurarsi che possano essere usati in caso di necessità.

Sicurezza delle Comunicazioni
Le informazioni trasferite su canali applicativi devono essere cifrate nel trasporto, ad esempio usando protocolli sicuri e non deprecati (TLS, https, ssh) o canali cifrati (VPN).

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.

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.

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 esportabili su richiesta.

Sicurezza fisica
Le server room e i datacenter devono essere ad accesso controllato e provvisti di misure di sicurezza fisica (antincendio, antiallagamento, controllo della temperatura, continuità elettrica).

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.

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".

ALLEGATO 2
MISURE DI SICUREZZA ORGANIZZATIVE RELATIVE AI DATI PERSONALI

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 referente la dimostrazione della conformità attraverso la compilazione della colonna "Compliance Status Partner".

Nel caso in cui l'ente 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 sicu\\rezza organizzative

Item #	Categoria	Controllo	Compliance status IIT (S/N/n.a.)	Compliance status PAP (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.	S	S	
2	Attribuzione di funzioni e compiti a soggetti autorizzati	Il personale interno che tratta dati personali è designato con apposito atto di nomina.	S	S	

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.	S	S	
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.	S	s	
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.	S	S	
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.	S	S	

2.2. Referente GDPR di PAP verso IIT

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

Gabriel, Zuchtriegel
gabriel.zuchtriegel@cultura.gov.it
+39 081 8575300

2.3. Referente GDPR di IIT verso PAP

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

GDPR Team
gdpr@iit.it
+39 010 28961