Sistemi Informativi S.r.l.
Sede Legale e Amministrativa
00148 Roma - Via Carlo Veneziani, 58
Telefono: 06/87793328
Fax: 06/52206164
www.sistinf.it

APPENDICE AL SUPPLEMENTO PER IL TRATTAMENTO DEI DATI PERSONALI

Contratto quadro SPC - Lotto 2 relativo alla fornitura di Servizi di cloud computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le pubbliche amministrazioni – Contratto esecutivo per l'adozione e l'utilizzo sicuro delle identità digitali del Sistema Pubblico di Identità Digitale (SPID) per il Cliente AGID.

Nella presente Appendice al Supplemento per il Trattamento dei Dati Personali (nel seguito per brevità "Appendice DPA"o "DPA Exhibit") si precisa il DPA per il Servizio identificato.

Trattamento dei Dati Personali

Sistemi Informativi tratterà i Dati Personali del Cliente e dei soggetti che accederanno al Customer Care per cittadini e imprese, come descritto nel Contratto e nel presente documento.

Durata del Trattamento dei Dati Personali

Sistemi Informativi tratterà i Dati Personali del Cliente per tutta la durata del Contratto.

Attività di trattamento

Le attività di Sistemi Informativi in relazione al Trattamento dei Dati Personali sono le seguenti:

- ricezione delle richieste di supporto

- analisi delle richieste di supporto

- formulazione del riscontro

- gestione della documentazione, nel rispetto della normativa in materia d protezione dei dati personali

Dati Personali trattati

Categorie di Interessati

Di seguito viene riportato un elenco delle Categorie di Interessati i cui Dati Personali possono essere generalmente trattati nell'ambito del Servizio:

- Cittadini che accederanno al Servizio

- Soggetti che ricoprono cariche sociali all'interno delle imprese che accederanno al Servizio

- Dipendenti e Collaboratori del Cliente

Categorie di Dati Personali

Tipologie di Dati Personali

Di seguito vengono elencate le Tipologie di Dati Personali che generalmente sono trattate nell'ambito del Servizio:

- dati anagrafici: nome, cognome;

- codice fiscale;

- dati di contatto: e-mail

Resta fermo che il Responsabile tratterà adeguatamente altresì tutti gli ulteriori dati personali che il richiedente indicherà volontariamente nel testo della propria richiesta di supporto.

Disposizioni Generali

Sistemi informativi tratterà i Dati Personali di tutti gli Interessati sopra elencati in conformità a quanto previsto nel Contratto. Data la natura dei Servizi, il Cliente riconosce che Sistemi informativi non è in grado di verificare il suddetto elenco di Categorie di Interessati. Pertanto, il Cliente è responsabile di fornire a Sistemi informativi informazioni complete, precise ed aggiornate sulle Categorie di Interessati contenute nell'elenco precedente.

Se le modifiche agli elenchi sopra detti richiedono modifiche rispetto al Trattamento concordato, il Cliente dovrà fornire Istruzioni Aggiuntive a Sistemi informativi come stabilito nel Contratto e nel DPA.

Misure Tecniche e Organizzative

Le misure tecniche e organizzative (technical and organizational measure, TOMs) applicabili al Servizio sono le seguenti:

Area di applicazione	id	Misure di protezione
1.1 Gestione documentazione	1.1.1	Mantenere registrazione delle approvazioni dei documenti sulla sicurezza dei dati e sulla privacy e renderla disponibile per scopi di report/audit.
1.1 Gestione documentazione	1.1.2	Creare e aggiornare i documenti sulla sicurezza dei dati e sulla privacy nei tempi stabiliti e revisionarli su base periodica
1.1 Gestione documentazione	1.1.3	Memorizzare e archiviare la documentazione di progetto in un repository protetto e sicuro
1.1 Gestione documentazione	1.1.4	Gestire i documenti in accordo con le direttive Corporate IBM
1.2 Gestione contratto e del subtrattamento	1.2.1	Creare e mantenere i documenti di progetto sulla sicurezza dei dati e sulla privacy che riflettono i requisiti richiesti dalle misure tecniche ed organizzative documentate negli appropriati accordi contrattuali
1.2 Gestione contratto e del subtrattamento	1.2.2	Valutare l'impatto delle modifiche al contratto sul trattamento dei Dati Personali del Cliente e aggiornare di conseguenza la documentazione sulla sicurezza dei dati e sulla privacy
1.2 Gestione contratto e del subtrattamento	1.2.4	Stipulare accordi scritti con tutti gli altri Subresponsabili del Trattamento (sub-processor) per imporre loro obblighi sostanzialmente similari a quelli stabiliti negli appropriati accordi contrattuali, in particolare per fornire sufficienti garanzie nell'attuare misure tecniche e organizzative adeguate

1.2 Gestione contratto e del subtrattamento	1.2.5	Definire e monitorare livelli di servizio (SLA) per i Subresponsabili (sub-processors) corrispondenti a quelli concordati col Cliente
1.2 Gestione contratto e del subtrattamento	1.2.6	Monitorare e documentare la conformità alle misure tecniche ed organizzative (TOMs) definite nell'Allegato al Supplemento per il Trattamento dei Dati Personali (DPA Exhibit)
1.3 Reviews, Assessments & Audits	1.3.1	Analizzare periodicamente i rischi di progetto relativi al trattamento dei dati personali
1.3 Reviews, Assessments & Audits	1.3.2	Implementare il modello di difesa su tre linee (Three Lines of Defense Model) dove le attività sono eseguite per indirizzare ogni linea in maniera appropriata sulla base dei rischi evidenziati da vari test e audit
1.3 Reviews, Assessments & Audits	1.3.3	Implementare e portare a termine piani di azioni derivanti da audit, test e verifiche sulla sicurezza
1.3 Reviews, Assessments & Audits	1.3.4	Rivedere periodicamente le normative, i processi e le istruzioni Sistemi Informativi relative alla sicurezza e aggiornarle se necessario
1.4 Gestione Rischi e Incident Management	1.4.1	Implementare un processo di gestione dei rischi
1.4 Gestione Rischi e Incident Management	1.4.2	Documentare e gestire i rischi di progetto e di trattamento dei dati in accordo con il processo di gestione dei rischi
1.4 Gestione Rischi e Incident Management	1.4.3	Implementare un processo di gestione degli incidenti di sicurezza per assicurare una immediata comunicazione, analisi d'impatto e efficaci azioni correttive (e preventive)
1.4 Gestione Rischi e Incident Management	1.4.4	Implementare un efficace piano di gestione delle emergenze assicurando un coinvolgimento adeguato dei legali IBM negli incidenti di sicurezza
1.4 Gestione Rischi e Incident Management	1.4.5	Implementare procedure per la prevenzione delle minacce per ridurre al minimo il rischio di violazioni della sicurezza
1.5 Project Management and People Management	1.5.1	Gestire gli aspetti relativi alla sicurezza dei dati e alla privacy utilizzando una metodologia di Project management
1.5 Project Management and People Management	1.5.2	Assicurare che i Dati Personali siano trattati esclusivamente in accordo con quanto stabilito nel Contratto e nel presente Supplemento per il Trattamento dei Dati Personali (DPA)
1.5 Project Management and People Management	1.5.3	Assicurare la disponibilità di adeguate competenze relative alla sicurezza dei dati e alla privacy
1.5 Project Management and People Management	1.5.4	Gestire la sicurezza dei dati e la privacy in accordo con le normative e le istruzioni organizzative della IBM Corporate che coprono i requisiti normativi per i Responsabili del Trattamento
1.5 Project Management and People Management	1.5.5	Definire ruoli e responsabilità per la sicurezza dei dati personali e delle informazioni secondo i livelli definiti dal Gruppo IBM
1.6 Classificazione, schemi, Inventario e Data Map delle informazioni.	1.6.1	Creare e gestire un inventario dei Dati Personali del Cliente e dei relativi elementi di sicurezza
1.6 Classificazione, schemi, Inventario e Data Map delle informazioni.	1.6.2	Creare e mantenere una lista delle procedure operative di sicurezza

1.7 Training	1.7.1	Eseguire formazione periodica specifica per il contratto relativa alla sicurezza dei dati e la privacy
1.7 Training	1.7.2	Eseguire formazione periodica specifica per il contratto relativa alla sicurezza dei dati e la privacy per i Subresponsabili (sub-processors)
1.7 Training	1.7.3	Eseguire a livello organizzativo formazione periodica sulla sicurezza dei dati e la privacy
1.7 Training	1.7.4	Eseguire formazione periodica per il corretto trattamento dei dati confidenziali
1.7 Training	1.7.5	Definire delle regole di gestione delle password in base alle nelle istruzioni IBM Corporate ed effettuare una formazione annuale per promuovere la consapevolezza dei dipendenti
2.2 Gestione degli accessi informatici (richiesta , approvazione, profilazione, modifica, revoca, rivalidazione)	2.2.1	Gestire l'accesso degli utenti all'ambiente tecnico di progetto
2.2 Gestione degli accessi informatici (richiesta , approvazione, profilazione, modifica, revoca, rivalidazione)	2.2.4	Limitare l'accesso ai sistemi aziendali da parte del personale del Cliente in base ad una necessità di business specifica ed approvata
2.2 Gestione degli accessi informatici (richiesta , approvazione, profilazione, modifica, revoca, rivalidazione)	2.2.6	Controllare l'accesso ai sistemi interni di Sistemi Informativi secondo le linee guida di IBM Corporate
3.2 Monitoraggio Network and Firewalls, Monitoraggio e gestione log di Sistema e Separazione ambienti	3.2.3	Gestire in modo sicuro l'accesso a ed attraverso la rete Sistemi Informativi
3.4 Tecniche di Data Protection Techniques (Encryption, Pseudoanonimizzazione, Anonimizzazione)	3.4.1	Adottare la crittografia, la pseudonimizzazione e / o l'anonimizzazione dei Dati Personali del Cliente nelle attività di trattamento, laddove applicabili
3.5 Attrezzature fisiche e utilizzo supporti	3.5.2	Implementare controlli di sicurezza per le workstation che trattano Dati Personali del Cliente
3.5 Attrezzature fisiche e utilizzo supporti	3.5.3	Implementare i controlli per il "mobile computing" e l'infrastruttura di comunicazione in conformità con le politiche di sicurezza IBM Corporate
3.5 Attrezzature fisiche e utilizzo supporti	3.5.4	Distruggere in modo sicuro le informazioni sensibili e il software in licenza prima del riutilizzo o dello smaltimento delle apparecchiature

Le seguenti misure tecniche e organizzative aggiuntive modificano le TOMs di cui sopra specificamente per il Servizio:

Protezione del Cliente da Phishing: Predisporre controlli di rilevamento e prevenzione di rete per aiutare a filtrare l'email phishing e i malware prima che raggiungano le workstation del Cliente gestite da SISTEMI INFORMATIVI in cui viene eseguito il trattamento di dati personali.

Crittografia dei Sistemi: Crittografare i dati personali memorizzati nei sistemi gestiti da SISTEMI INFORMATIVI

Crittografia dei Backup: Crittografare i dati personali sui supporti portatili di backup utilizzati per eseguire il backup dei dati dai sistemi del Cliente gestiti da SISTEMI INFORMATIVI.

Proteggere i backup: Mantenere i supporti di backup che contengono dati personali in un contenitore chiuso quando non sono in uso.

Blocco Schermo: Configurare i blocchi schermo per limitare l'accesso alle workstation non presidiate del Cliente gestite da SISTEMI INFORMATIVI, in cui viene eseguita la memorizzazione, il trattamento o l'accesso dei dati personali.

Test del Backup: Convalidare l'integrità del processo di backup periodicamente eseguendo il test di ripristino dei dati.

Risposta agli Incidenti: Mantenere una capacità di investigazione e reazione ad incidenti di sicurezza in ambito IT sufficienti per la conformità con le normative applicabili, incluse quelle riguardanti la notifica di violazioni dei dati.

Test dei Software: Testare i nuovi software (incluse le patch, i service pack e altri aggiornamenti) in un ambiente non di produzione prima di passarlo alla produzione su sistemi del Cliente gestiti da SISTEMI INFORMATIVI in cui viene eseguito il trattamento di dati personali.

Applicazione patch sulle Applicazioni gestite da SISTEMI INFORMATIVI: Applicare le patch al middleware gestito da SISTEMI INFORMATIVI e alle applicazioni sui sistemi del Cliente gestiti da SISTEMI INFORMATIVI in cui viene eseguito il trattamento di dati personali.

Applicazione patch sulle Applicazioni gestite dal Cliente: Applicare le patch al middleware gestito dal cliente e alle applicazioni sui sistemi del Cliente gestiti da SISTEMI INFORMATIVI in cui viene eseguito il trattamento di dati personali.

Limitazione Accessi: Limitare l'accesso ai dati personali nei file system, nelle condivisioni di rete, applicazioni e database, utilizzando le "access control list" nei sistemi del Cliente gestiti da SISTEMI INFORMATIVI.

Autenticazione a più Fattori ID amministrativi: Richiedere l'autenticazione a più fattori per l'accesso di tutti gli amministratori di sistema ai sistemi del Cliente gestiti da SISTEMI INFORMATIVI in cui viene eseguito il trattamento di dati personali.

Crittografia File ID: Eseguire la crittografia o l'algoritmo hash su tutti i file di autenticazione e garantire che tali file siano accessibili solo agli account root o amministratori nei sistemi del Cliente gestiti da SISTEMI INFORMATIVI in cui viene eseguito il trattamento di dati personali.

Sistemi informativi ha ottenuto le seguenti certificazioni di sicurezza standard, i sigilli e i marchi dei dati personali per verificare, valutare e convalidare regolarmnente l’efficacia dell TOMs:

ISO 9001

ISO 27001

ISO 20000

Verifica (“Audit”)

La conduzione dell'audit sarà soggetta alle procedure di audit concordate fra le Parti, secondo quanto stabilito nel Contratto.

Cancellazione e restituzione dei Dati Personali al Cliente

Sistemi informativi, su richiesta del Cliente, restituirà i Dati Personali che siano eventualmente ancora trattati da Sistemi informativi entro il periodo concordato con il Cliente ovvero li cancellerà.

Subresponsabili

Sistemi informativi può utilizzare il/i seguente/i Subresponsabile/i per il Trattamento dei Dati Personali, i quali si trovano in un Paese UE:

Nome del Subresponsabile	Con sede nel Paese

Trattamento dei Dati Transfrontaliero

Non ricorre flusso di dati transfrontaliero. Le Clausole Contrattuali Standard UE non sono richieste per l'erogazione del Servizio.

Responsabile della Protezione dei Dati e altri Titolari del Trattamento dei Dati

Il Cliente è responsabile di fornire informazioni complete, esatte e aggiornate riguardanti i suoi responsabili della protezione dei dati (Data Privacy Officers) e ogni altro Titolare del Trattamento dei Dati (inclusi quelli riguardanti i loro responsabili della protezione dei dati) tramite e-mail ai referenti contrattuali.

Il DPO di Gruppo per IBM Company è disponibile al seguente indirizzo email ChiefPrivacyOffice@ca.ibm.com

Data Protection Officer (Responsabile della Protezione dei Dati Personali) del Cliente

Nome: Raffaella Vai

Dettagli di contatto: responsabileprotezionedati@agid.gov.it

Referente Sistemi Informativi per la Privacy

Il contatto sulla privacy Sistemi Informativi è disponibile al seguente indirizzo email ***Tutelaprivacy@sistinf.it***