

INVITALIA

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

INV-INV - Prot n. 0299770 del 01-12-2021 13.57



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

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, modifica 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 protection 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'istruzione 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 "Gestione 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 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 assicurandone 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.

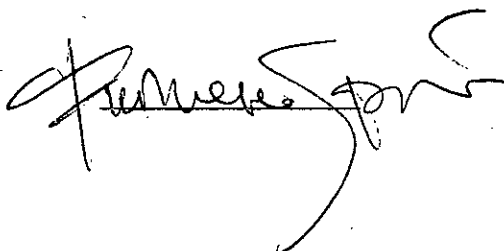
Misure:

- 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 fornitore, 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 attività che comportano un trattamento di dati per conto di INVITALIA.

Roma, 29/11/2021

Il DPO

Dr. Francesco Sprovieri



Sistemi Informativi

Dr. Alessio Antolini

