AGID
Agenzia per l'Italia Digitale

# Analisi del rischio
# sulla protezione dei dati personali

## Single Digital Gateway
## Italia

# I. Contesto

## 1. Panoramica del trattamento

La presente analisi del rischio concerne il trattamento dei dati personali svolto mediante lo sportello digitale unico (*Single Digital Gateway* - di seguito SDG) per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi nonché mediante il correlato sistema tecnico per lo scambio transfrontaliero automatizzato di prove, di cui al Regolamento (UE) 2018/1724 del Parlamento europeo e del Consiglio del 2 ottobre 2018, con specifico riferimento all'Italia.

### 1.1. Base giuridica del trattamento

La base giuridica del trattamento è individuata come segue:

- Regolamento (UE) 2018/1724 del Parlamento europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012;
- Regolamento di esecuzione (UE) 2022/1463 della Commissione del 5 agosto 2022 che definisce le specifiche tecniche e operative del sistema tecnico per lo scambio transfrontaliero automatizzato di prove e l'applicazione del principio "una tantum" a norma del regolamento (UE) 2018/1724 del Parlamento europeo e del Consiglio;
- Il "Piano Nazionale di Ripresa e Resilienza" presentato dall'Italia alla Commissione europea in data 30 giugno 2021 e valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021, notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21 del 14 luglio 2021 che individua l'Agenzia per l'Italia Digitale quale soggetto attuatore del sub-investimento 1.3.2 - Single Digital Gateway e, pertanto, soggetto gestore delle componenti nazionali italiane.

### 1.2. Finalità del trattamento

Il trattamento è volto all'istituzione e al funzionamento del SDG, al fine di consentire ai cittadini e alle imprese un facile accesso alle informazioni, alle procedure e ai servizi di assistenza e di risoluzione dei problemi di cui necessitano per l'esercizio dei propri diritti nel mercato interno europeo.

### 1.3. Ruoli e conseguenti responsabilità

L'art. 33 del Regolamento di esecuzione (UE) 2022/1463 prevede che "le rispettive autorità competenti degli Stati membri, nella loro qualità di richiedenti prove o fornitori di prove, agiscono in qualità di titolari del trattamento, quali definiti all'articolo 4, punto 7, del regolamento (UE) 2016/679, e come ulteriormente specificato negli articoli 34 e 35 del presente regolamento".

L'art. 35, par. 2, del medesimo Regolamento di esecuzione (UE) 2022/1463 prevede che "Quando mette a disposizione lo spazio di anteprima in conformità all'articolo 15, paragrafo 1, lettera b), punto ii), del presente regolamento, una piattaforma di intermediazione è considerata un responsabile del trattamento che agisce per conto del fornitore di prove in conformità all'articolo 4, punto 8, del regolamento (UE) 2016/679".

Il "Piano Nazionale di Ripresa e Resilienza" individua l'Agenzia per l'Italia Digitale quale soggetto attuatore del sub-investimento 1.3.2 - Single Digital Gateway e, pertanto, soggetto gestore delle componenti nazionali italiane.

Alla luce di quanto stabilito dalla normativa, di quanto discusso con il Garante per la protezione dei dati personali al momento della prima impostazione dell'architettura della piattaforma di intermediazione e sulla base dello specifico atto di nomina da formalizzarsi ai sensi dell'art. 28 GDPR, le responsabilità del trattamento sono così individuate:

| | |
|---|---|
| **Titolari del trattamento** | Le **Autorità competenti** ai sensi dell'art. 3, n. 4) del Regolamento istitutivo, sia in qualità di fornitori di prove sia di richiedenti prove ai sensi dell'art. 1, nn. 2) e 3) del Regolamento di esecuzione |
| **Responsabile del trattamento per le componenti nazionali SDG** | **Agenzia per l'Italia Digitale**<br>C.F.: 97735020584<br>Via Liszt n. 21 - 00144 Roma<br>Tel.: 06/852641<br>PEC: protocollo@pec.agid.gov.it |
| **Sub-responsabile del trattamento per l'interoperabilità a mezzo della PDND** | **PagoPA S.p.A.**<br>C.F. e P. IVA: 15376371009<br>Piazza Colonna n. 370 - 00187 Roma<br>pagopa@pec.governo.it |

| | |
|---|---|
| **Sub-responsabile del trattamento per la gestione applicativa e infrastrutturale** | **Accenture S.p.A.**<br>P. IVA: 13454210157<br>Via Privata Nino Bonnet n. 10 - 20154 Milano<br>Tel.: 02/77758090<br>PEC: accenture@legalmail.it |
| | **Accenture Technology Solutions S.r.l.**<br>P. IVA: 03646450969<br>Via Privata Nino Bonnet n. 10 - 20154 Milano<br>Tel.: 02/77751111<br>PEC: accenture.technology.solutions@legalmail.it |
| | **Spindox S.p.A.**<br>P. IVA: 09668930010<br>Via Bisciglie n. 76 - 20152 Milano<br>PEC: spindox@legalmail.it |
| **Sub-responsabile del trattamento per l'hosting** | **Almaviva – The Italian innovation company S.p.A.**<br>P. IVA: 08450891000<br>Via di Casal Boccone 188-190 – 00137 Roma<br>PEC: almaviva@pec.almaviva.it |
| **Sub-responsabili del trattamento per l'hosting (per Almaviva)** | **AMAZON WEB SERVICES EMEA SARL**<br>P.IVA: LU 26888617<br>38 avenue John F. Kennedy, L-1855 Lussemburgo<br><br>**AMAZON ITALIA SERVICES SRL**<br>P.IVA 10119840964<br>viale Monte Grappa 3/5 - 20124 Milano<br>PEC: amazonwebservicesemea@legalmail.it |

### 1.4. Standard applicabili

Gli standard applicati al trattamento in materia di protezione dei dati sono i seguenti:

- ISO IEC 27001
- ISO IEC 27701

## 2. Ciclo di vita del trattamento dei dati personali: descrizione funzionale

Il nodo italiano SDG è costituito da sei componenti applicative:

- Catalogo dei Servizi;

- Evidence broker;
- Data service directory;
- Architecture common services;
- Access point;
- Preview space.

Fra tali componenti, unicamente sulle seguenti quattro sono effettuate attività che comportano il trattamento di dati personali: Catalogo dei Servizi, Architecture common services, Access point, Preview space.

Di seguito vengono riportati e analizzati i processi applicativi che prevedono il trattamento di dati personali.

## 2.1. Registrazione dei referenti AgID e degli utenti afferenti le Autorità competenti

AGID provvede a registrare sul Catalogo dei Servizi i propri referenti preposti alla gestione delle componenti nazionali di SDG, distinti in due profili con autorizzazioni differenti: il c.d. "Amministratore Globale" e il c.d. "Contributore AgID".

Al momento del primo approccio con SDG, le Autorità competenti inviano ad AGID - al di fuori delle componenti SDG, a mezzo PEC - gli estremi degli utenti referenti dell'Autorità stessa, distinti in due profili con autorizzazioni differenti: il c.d. "Amministratori Ente" e il c.d. "Contributore Ente".

Si specifica che il Catalogo dei Servizi è destinato unicamente alle Autorità competenti italiane.

Nella tabella seguente viene riassunto l'operatività dei profili previsti dall'applicazione in relazione agli oggetti gestiti dal backoffice del Catalogo dei servizi. L'operatività degli utenti afferenti alle Autorità competenti, è limitata agli oggetti di proprietà dell'Autorità competente.

| | Amministratore globale/AgID | Amministratore ente | Contributore Ente | Contributore AgID |
|---|---|---|---|---|
| **Momenti di vita** | Visualizzare, creare, modificare, eliminare | Visualizzare | Visualizzare | Visualizzare |
| **Ambiti** | Visualizzare, creare, modificare, eliminare | Visualizzare | Visualizzare | Visualizzare |

| | | | | |
|---|---|---|---|---|
| **Procedure** | Visualizzare, creare, modificare, eliminare | Visualizzare | Visualizzare | Visualizzare |
| **Procedimenti amministrativi** | Visualizzare, creare, modificare, eliminare | Visualizzare, creare, modificare, eliminare | Visualizzare, richiesta di creazione, richiesta di modifica, richiesta di eliminazione | Visualizzare, richiesta di creazione, richiesta di modifica, richiesta di eliminazione |
| **Novità** | Visualizzare, creare, modificare, eliminare | Visualizzare, creare, modificare, eliminare | Visualizzare, richiesta di creazione, richiesta di modifica, richiesta di eliminazione | Visualizzare, richiesta di creazione, richiesta di modifica, richiesta di eliminazione |
| **Utenti** | Visualizzare, creare, modificare, eliminare | Visualizzare, creare, modificare, eliminare per gli utenti afferenti agli enti | N/A | N/A |
| **FAQ** | Visualizzare, creare, modificare, eliminare | Visualizzare, creare, modificare, eliminare | Visualizzare, richiesta di creazione, richiesta di modifica, richiesta di eliminazione | Visualizzare, richiesta di creazione, richiesta di modifica, richiesta di eliminazione |
| **Soggetti erogatori** | Visualizzare, creare, modificare, eliminare | Visualizzare, creare, modificare, eliminare | N/A | N/A |
| **Servizi di trasmissione prova** | Visualizzare, creare, modificare, eliminare | Visualizzare | N/A | N/A |
| **Documentazione** | Visualizzare | Visualizzare | Visualizzare | Visualizzare |
| **Trattamento dati** | Visualizzare, creare, eliminare | Visualizzare, creare, eliminare | Visualizzare, creare, eliminare | Visualizzare, creare, eliminare |

*Tabella 1 - Operatività dei profili in relazione agli oggetti mantenuti sul Catalogo dei servizi*

Ricevuti gli estremi di riconoscimento di tali referenti delle Autorità, l'Amministratore globale esegue l'accesso ad apposita funzionalità del backoffice del Catalogo dei Servizi al fine di registrare i referenti delle Autorità distinti nei due profili sopra citati.

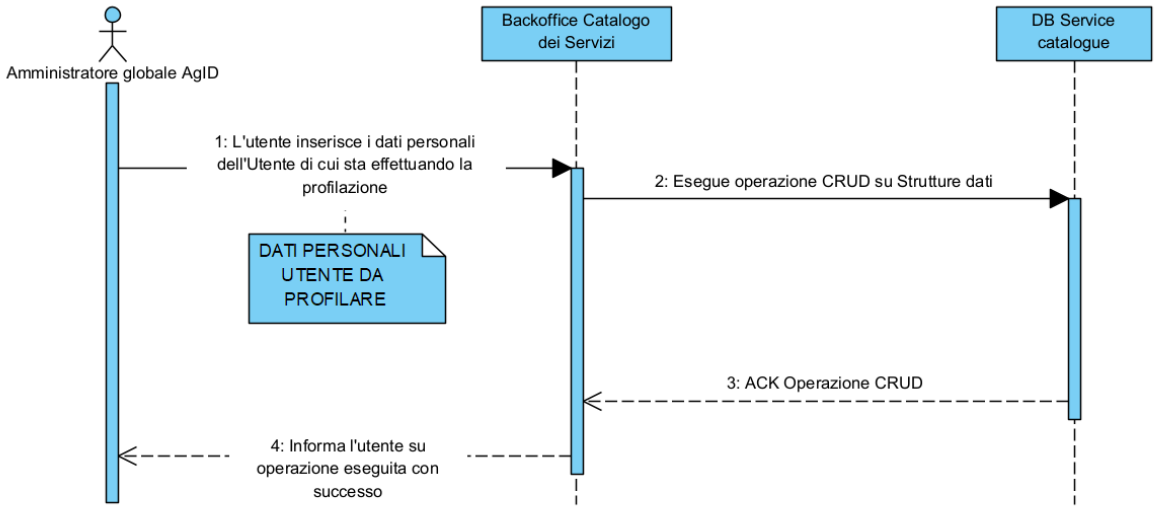



*Figura 1 - Processo di registrazione sul sistema dei referenti di AgID e delle Autorità competenti*

**Dati personali trattati**: nome, cognome, codice fiscale nonché indirizzo e-mail istituzionale;

**Finalità**: i dati personali sono trattati per la registrazione dei referenti sul Catalogo dei Servizi e la successiva verifica di corrispondenza di tale set di dati con quello che sarà acquisito in fase di login dei referenti mediante la propria identità digitale SPID e CIE (cfr. successivo paragrafo); l'indirizzo di posta elettronica è richiesto per esigenze di contatto. Il processo è strutturato in modo da trattare il set minimo di dati necessari all'identificazione in maniera univoca dell'utente e alle esigenze di contatto.

**Conservazione**: i dati personali sono conservati sul database del Catalogo dei servizi per il tempo in cui l'utente resta referente dell'AgID o dell'Autorità competente e in ogni caso – con riferimento ai referenti delle Autorità competenti - per la durata dell'accordo stipulato fra Autorità e AgID in qualità di gestore delle componenti nazionali di SDG. A seguito della sostituzione del referente, nel caso in cui non siano state eseguite operazioni di creazione, modifica, eliminazione di dati, i dati personali di quest'ultimo sono eliminati. In caso contrario, i dati personali permangono per 5 anni dalla decadenza dell'Accordo stesso, a garanzia di eventuali esigenze probatorie.

## 2.2. Login e navigazione dei referenti di AgID e delle Autorità competenti

Al fine di poter operare sulle componenti in base ai propri poteri, i referenti di AgID e delle Autorità competenti eseguono l'accesso al backoffice del Catalogo dei Servizi tramite uno IAM che esegue la validazione dell'identità digitale del referente mediante SPID e CIE.

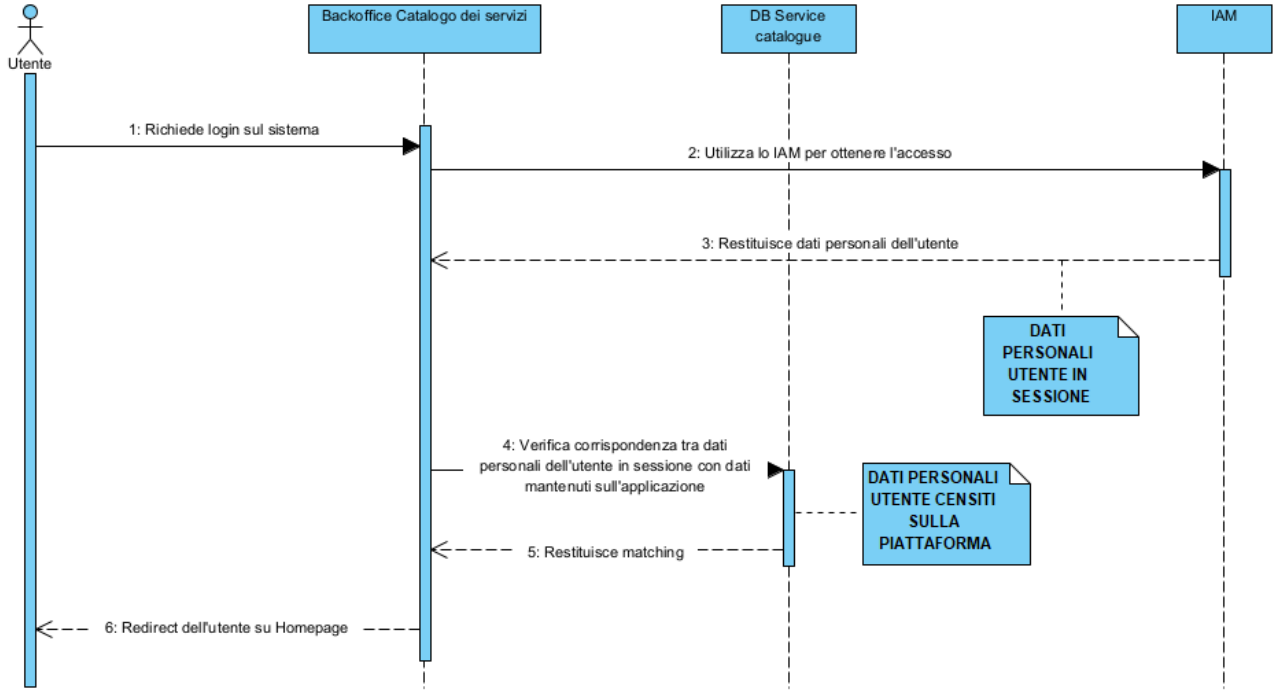



*Figura 2 – Processo di login e navigazione del referente*

**Dati personali**: Codice identificativo, Nome, Cognome, Data di nascita, Codice fiscale mediante lo strumento di identificazione utilizzato, nonché e-mail istituzionale mediante matching con i dati già registrati sul Catalogo dei Servizi.

**Finalità**: i dati personali dei referenti sono trattati per l'identificazione degli stessi al momento del login sul Catalogo dei Servizi e per consentire al backoffice del Catalogo dei Servizi la verifica della corrispondenza tra i dati personali registrati *ab origine* (vedi par. 2.1) sul Catalogo e quelli ottenuti mediante l'accesso con identità digitale.

**Conservazione**: in caso di esito negativo della verifica sopra citata, i dati personali sono immediatamente cancellati; in caso di esito positivo, i dati personali ottenuti mediante

l'accesso con identità digitale sono mantenuti unicamente per il tempo della sessione per consentire la piena operatività del referente sul Catalogo dei Servizi e cancellati al termine della sessione stessa.

## 2.3 Designazione di AgID quale responsabile del trattamento dei dati

L'utente con profilo Amministratore globale e quello con profilo di Amministratore Ente stipulano l'atto di nomina di AgID quale responsabile del trattamento dei dati personali ai sensi degli artt. 4, n. 8) e 28 del GDPR.

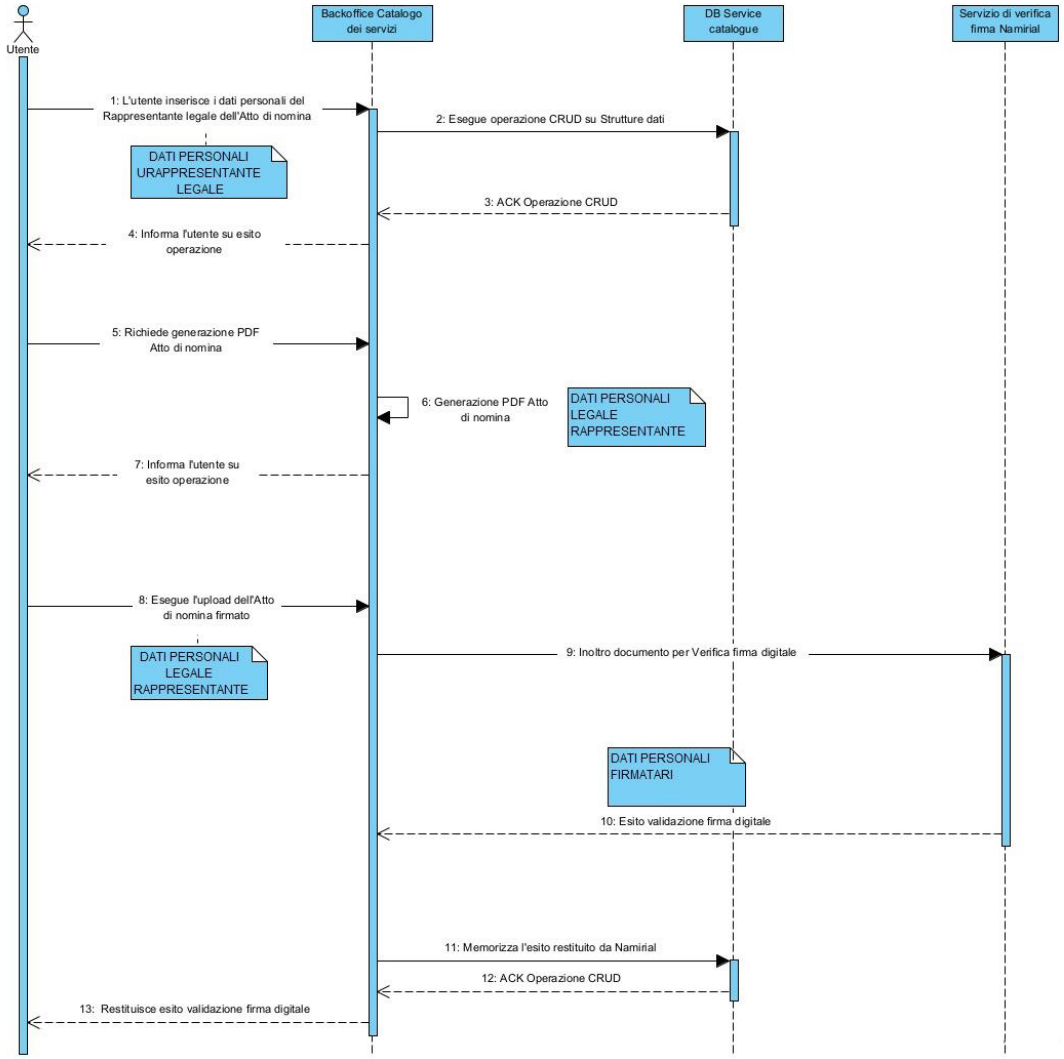



*Figura 1 – Processo di gestione atto di nomina del responsabile del trattamento dei dati*

**Dati personali trattati**: oltre ai dati sopra citati dell'Amministratore globale e dell'Amministratore Ente, sono trattati altresì il nome, il cognome, il codice fiscale del Direttore Generale pro tempore di AgID e il nome, il cognome e il codice fiscale del legale rappresentante e degli eventuali diversi firmatari per conto dell'Autorità competente. Si specifica che il codice fiscale è utilizzato esclusivamente al fine di verificare la correttezza delle firme digitali apposte.

**Finalità**: i dati personali sono trattati per la stipula dell'atto di nomina ex art. 28 GDPR.

**Conservazione**: i dati personali inseriti sul Catalogo dei Servizi per la sottoscrizione dell'atto di nomina sono conservati sul relativo database; i file degli atti di nomina sono conservati su file system (cloud di Amazon, Web Services S3, con database sul territorio nazionale).

### 2.4 Scambio di prove fra Autorità competenti

L'iter di scambio di una prova su SDG inizia con la richiesta di accesso di un utente sul procedure portal di un'Autorità competente, presso la quale intende utilizzare un servizio online.

#### 2.4.1. Richiesta di accesso a un servizio online

L'utente accede al procedure portal dell'Autorità competente autenticandosi mediante un valido strumento di identificazione:

- qualora l'utente sia italiano o comunque in possesso di SPID/CIE, l'accesso è consentito mediante uno di tali strumenti;
- qualora l'utente sia transfrontaliero, l'accesso è consentito mediante eIDAS.

In tale secondo caso, laddove il servizio online richieda necessariamente l'indicazione del codice fiscale dell'utente, il procedure portal dell'Autorità competente, al fine di completare il processo di identity matching, può utilizzare il servizio di validazione del codice fiscale messo a disposizione dall'Agenzia delle entrate ed esposto su Architecture common service SDG IT:

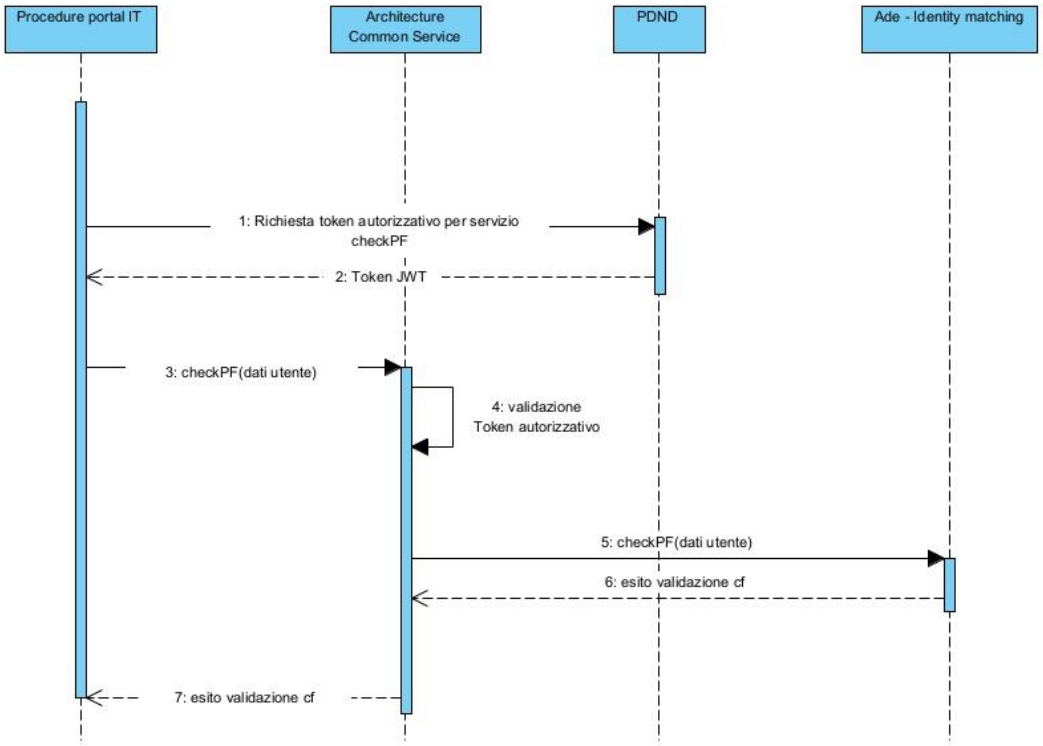



*Figura 4 - Servizio di validazione codice fiscale reso dall'Agenzia delle entrate*

Come esplicato nel grafico sopra riportato, i dati personali dell'utente transfrontaliero sono comunicati dal procedure portal dell'Autorità competente al nodo italiano di SDG tramite apposita API esposta da Architecture common service SDG IT e, successivamente, sono da questi inoltrati all'apposita API esposta dall'Agenzia delle entrate.

Il set di dati, comprensivo dell'esito della validazione, è successivamente trasmesso dall'Agenzia delle entrate al nodo SDG che, a sua volta, lo invia all'Autorità competente che ha richiesto la validazione.

In tali casistiche di utilizzo del servizio di validazione del codice fiscale, il nodo di SDG tratta i seguenti dati personali dell'utente transfrontaliero, in quanto richiesti dall'Agenzia delle entrate per l'erogazione del servizio di validazione: codice fiscale, cognome, nome, genere, data di nascita, comune di nascita, provincia di nascita, Stato di nascita, tipologia supporto, identificativo supporto.

Tali dati personali - sia in entrata sia in uscita, comprensivi dell'esito fornito dall'Agenzia delle entrate - non sono mantenuti in sessione né conservati sull'architettura.

### 2.4.2. Attestazione della rappresentanza legale in caso di utente soggetto giuridico

Qualora l'utente sia nazionale sia transfrontaliero sia un soggetto giuridico, il nodo italiano SDG mette a disposizione il servizio di attestazione della rappresentanza legale, reso dall'Unione Italiana delle Camere di Commercio, Industria, Artigianato e Agricoltura

(Unioncamere) ed esposto su Architecture common service SDG IT.
Tramite apposita API esposta da Architecture common service SDG IT, SDG veicola il messaggio per Unioncamere in cui sono riportati: codice fiscale del rappresentante legale del soggetto giuridico, codice fiscale del soggetto giuridico, codice IPA, identificativo univoco del procedimento amministrativo. La risposta ottenuta da Unioncamere, contente lo stesso set di dati personali con l'aggiunta dell'esito della validazione (espresso con valore booleano), viene inoltrata all'Autorità competente che ha richiesto l'attestazione.
I dati contenuti nel messaggio non vengono mantenuti in sessione né conservati sull'architettura.

### 2.4.3. Intermediazione del nodo italiano di SDG

Qualora l'Autorità competente necessiti di una prova per l'erogazione del servizio online che l'utente ha chiesto di utilizzare, il procedure portal dell'Autorità medesima comunica tale richiesta all'Architecture Common Services SDG IT che, a sua volta, la inoltra all'Autorità competente in possesso di tale prova.
Tale Autorità competente, in possesso della prova necessaria per l'erogazione del servizio online a cui ha effettuato l'accesso l'utente, estrae la prova e la consegna all'Architecture Common Services SDG IT.
Il nodo mantiene la prova sulla propria piattaforma di intermediazione, permettendo all'Autorità competente che l'ha richiesta – mediante un'apposita chiamata ai sever del nodo SDG - di procedere al recupero della prova, potendo così finalizzare l'erogazione del servizio a favore dell'utente.
Nel processo di intermediazione, il nodo italiano di SDG interviene nel trattamento dei dati personali contenuti nella prova oggetto di scambio.
Lo schema infra riportato illustra l'iter più nel dettaglio:

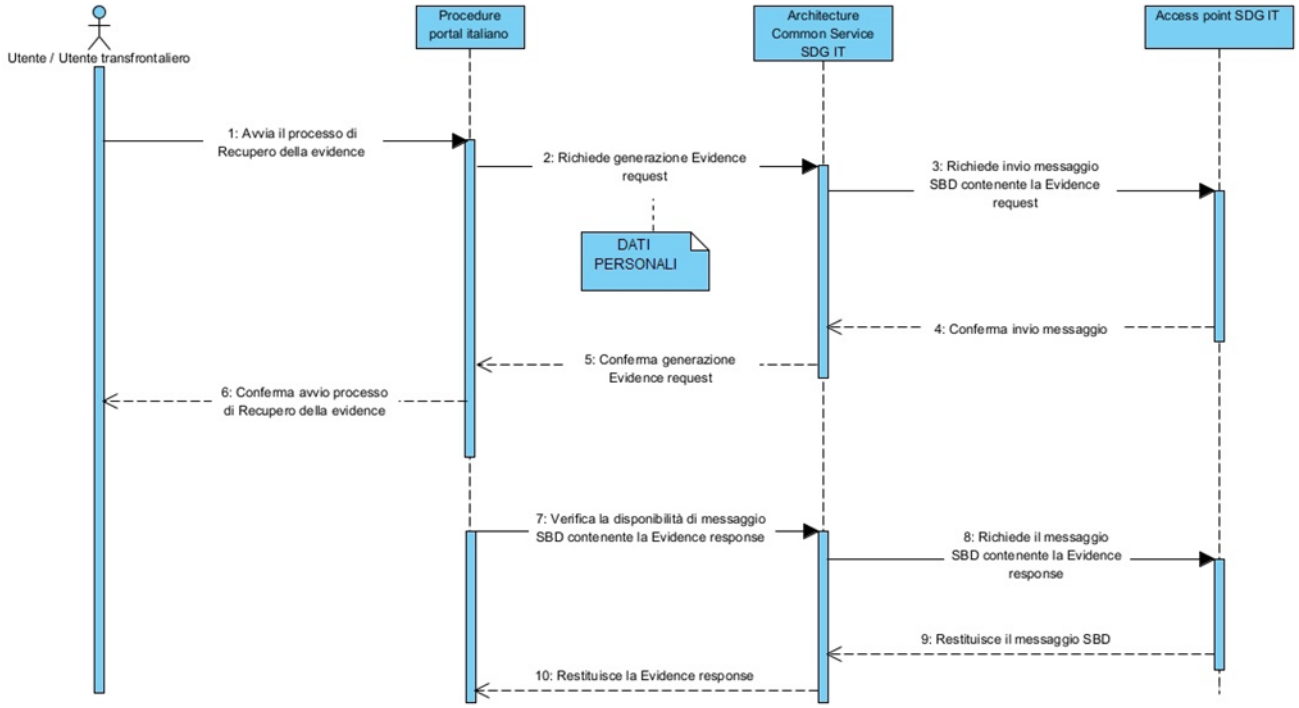



*Figura 5 - Iter di recupero di una prova*

**Dati personali trattati**: qualsiasi dato personale contenuto nella prova oggetto di scambio.

**Finalità**: i dati personali sono trattati unicamente per consentire lo scambio della prova fra le due Autorità competenti mediate SDG, per il tempo strettamente necessario al transito della medesima e al recupero da parte dell'Autorità richiedente.

**Conservazione**: i dati dell'utente, compresa la prova, permangono sulla piattaforma di intermediazione per la durata necessaria al completamento del processo di recupero e/o, in ogni caso, cancellati entro 12 mesi dalla ricezione della prova.

### 2.4.4. Lo spazio di anteprima

Lo spazio di anteprima è predisposto per fornire all'utente la possibilità di visionare in anteprima la prova, finalizzando o rifiutando il recupero della stessa, e il suo utilizzo si configura ordinariamente come una facoltà rimessa all'Autorità competente che richiede la prova.

Per consentire l'anteprima, il nodo prevede che l'Autorità competente richiedente la prova indirizzi l'utente, mediante un apposito link, sullo spazio di anteprima, presso cui l'utente è tenuto ad autenticarsi mediante SPID/CIE o eIDAS.

Il ricorso allo spazio di anteprima prevede lo scambio di una serie di messaggi correlati di tipo

eDelivery AS4 tra Autorità competente richiedente la prova, l'Autorità competente in possesso della prova e lo spazio di anteprima, come da iter infra descritto:

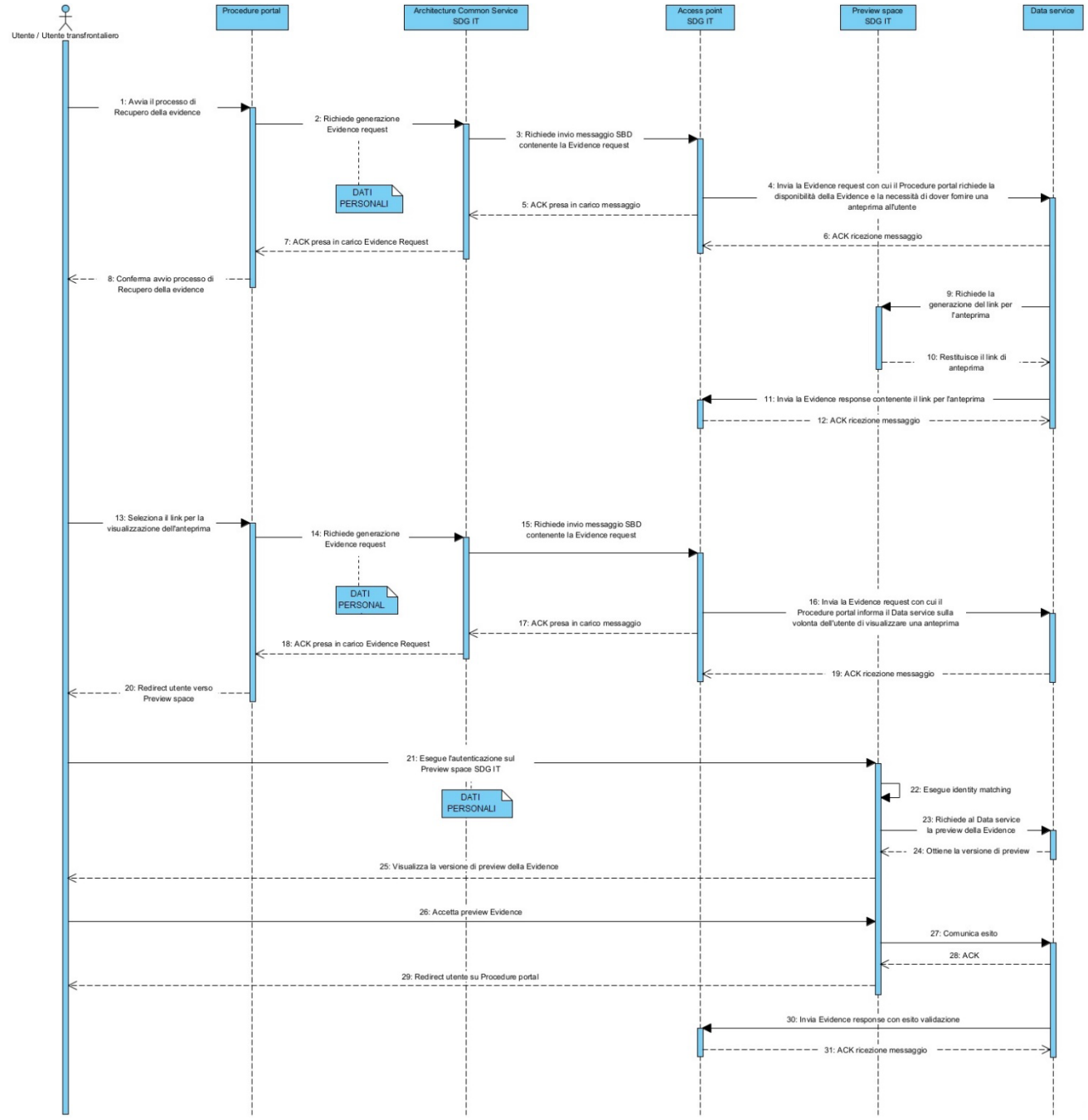



*Figura 6 - Processo applicativo dell'anteprima di una prova*

Lo spazio di anteprima si configura, invece, quale passaggio obbligatorio nei casi in cui l'Autorità competente in possesso della prova necessiti di attributi ulteriori per il rilascio della stessa: in tale contesto, l'Autorità in possesso della prova ne fa esplicita richiesta al nodo SDG che lo comunica all'Autorità richiedente la prova. Tale Autorità reindirizza l'utente presso lo spazio di anteprima predisposto dal nodo SDG sulla propria

piattaforma di intermediazione.
L'utente, autenticatosi sullo spazio di anteprima, può inserire gli attributi richiesti che il nodo SDG provvede a trasmettere all'Autorità in possesso della prova. Ottenuti gli attributi ulteriori, l'Autorità competente in possesso della prova procede al rilascio di questa come da precedente paragrafo.
Si specifica che, qualora sullo spazio di anteprima si debba autenticare un utente transfrontaliero, il nodo SDG utilizza il servizio di validazione del codice fiscale sopra descritto al paragrafo 2.4.1.

**Dati personali richiesti per l'autenticazione dell'utente sullo spazio di anteprima**:
a) utente italiano o in possesso di SPID/CIE: Codice identificativo, Nome, Cognome, Data di nascita, Sesso, Codice fiscale, Indirizzo di posta elettronica, acquisiti mediante lo strumento di autenticazione SPID/CIE;
b) utente transfrontaliero: Nome, Cognome, Data di nascita, Identificativo univoco nel caso di persona fisica: Nome entità legale, Identificativo univoco nel caso di persona giuridica. I dati menzionati vengono acquisiti mediante lo strumento di autenticazione eIDAS.
È trattato, inoltre, ogni altro dato personale inserito volontariamente dall'utente al fine di comunicare i richiesti attributi ulteriori al fine del recupero della prova.

**Finalità**: i dati sono richiesti per l'autenticazione dell'utente sullo spazio di anteprima reso disponibile dal nodo SDG e per a comunicazione degli attributi ulteriori all'Autorità in possesso della prova che ne abbia fatto richiesta.

**Conservazione**: i dati personali e la prova oggetto di anteprima sono trattati solo per il tempo della sessione e poi immediatamente cancellati.

# 3. Dati, processi e risorse a supporto

## 3.1. Categorie di interessati e relative tipologie di dati personali trattati

| Categorie di interessati | Categorie di dati personali trattati |
|---|---|
| Referenti delle Autorità competenti di cui all'art. 3, n. 4) del Regolamento istitutivo | - Registrazione: nome, cognome, codice fiscale, indirizzo e-mail istituzionale.<br><br>- Login: codice identificativo, Nome, Cognome, Data di nascita, Codice fiscale mediante lo strumento di identificazione utilizzato, nonché e-mail istituzionale. |
| Utenti, ai sensi dell'art. 3, nn. 1) e 2) del Regolamento istitutivo | - Processo di scambio delle prove: qualsiasi dato personale contenuto nella prova oggetto di scambio.<br><br>- Spazio di anteprima:<br>a) utente italiano o in possesso di SPID/CIE: Codice identificativo, Nome, Cognome, Data di nascita, Sesso, Codice fiscale, Indirizzo di posta elettronica, acquisiti mediante lo strumento di autenticazione SPID/CIE;<br>b) utente transfrontaliero: Nome, Cognome, Data di nascita, Identificativo univoco nel caso di persona fisica; Nome entità legale, Identificativo univoco nel caso di persona giuridica. I dati menzionati vengono acquisiti mediante lo strumento di autenticazione eIDAS.<br>Inoltre:<br>- ogni dato personale inserito volontariamente dall'utente al fine di comunicare i richiesti attributi ulteriori al fine del recupero della prova; |

| Categorie di interessati | Categorie di dati personali trattati |
|---|---|
| | - qualsiasi dato personale contenuto nella prova oggetto di scambio. |

### 3.2. Categorie di destinatari dei dati personali

Nessun dato personale è oggetto di trasferimento a destinatari diversi dalle Autorità competenti.

Non è contemplato alcun trasferimento in Paesi extraeuropei o a organizzazioni internazionali, al di fuori dell'utilizzo di servizi resi da fornitori extraeuropei nel rispetto delle garanzie di cui alla decisione di adeguatezza adottata dalla Commissione europea in data 10 luglio 2023 e con database ubicati nel territorio nazionale.

### 3.3. Periodo di conservazione dei dati personali

Nella tabella seguente vengono riportate le specifiche di conservazione, archiviazione e distruzione per ogni attività di trattamento dei dati personali di cui alla "sezione I – Capitolo 2 "Ciclo di vita del trattamento dei dati personali: descrizione funzionale".

| TRATTAMENTO DATI PERSONALI | PERIODO DI CONSERVAZIONE | SUPPORTO PER LA CONSERVAZIONE |
|---|---|---|
| Registrazione referenti su back office catalogo servizi | I dati vengono cancellati immediatamente in caso di sostituzione del referente o conservati per 5 anni dalla decadenza dell'Accordo con l'Autorità competente nel caso in cui il referente abbia eseguito operazioni di creazione, modifica, eliminazione di oggetti. | Database Catalogo dei servizi (Amazon Relational Database Services (RDS) con engine PostgreSQL) |
| Login e navigazione referenti su catalogo servizi | In caso di esito negativo di matching tra dati presentati in fase di login e dati registrati ab origine sul Catalogo dei servizi, i dati personali vengono immediatamente cancellati. In caso di esito positivo, sono mantenuti unicamente per la durata della sessione di navigazione. | N/A |
| Stipula atto di designazione AgID ex art. 28 GDPR | I dati sono conservati per 5 anni dalla decadenza della Convenzione. | Database Catalogo dei servizi (Amazon Relational Database Services (RDS) con engine PostgreSQL) |

| | | |
|---|---|---|
| | | Filesystem Catalogo dei servizi (Amazon S3 (Simple Storage Service) |
| Servizio validazione codice fiscale | I dati personali non sono mantenuti in sessione né conservati sull'architettura. | N/A |
| Attestazione rappresentante legale | I dati personali non sono mantenuti in sessione né conservati sull'architettura. | N/A |
| Intermediazione o processo scambio prova | I dati dell'utente, compresa la prova, permangono sulla piattaforma di intermediazione per la durata necessaria al completamento del processo di recupero e/o, in ogni caso, cancellati entro 12 mesi dalla ricezione della prova | Database Access Point (Amazon Relational Database Services (RDS) con engine MySQL) |
| Preview space | I dati personali dell'utente e la prova recuperata sono trattati solo per il tempo della sessione e poi immediatamente cancellati. | N/A |

### 3.4. Risorse di supporto ai dati personali

I dati trattati dal nodo italiano SDG sono ospitati sui database di AWS, mediante servizi Platform As A Service e Serverless.

Di seguito una descrizione delle risorse utilizzate per la gestione dei dati personali nelle varie fasi del processo di utilizzo di SDG:

- Amazon Relational Database Services (RDS) con engine PostgreSQL

Tale servizio ospita il Database del Catalogo dei Servizi.

RDS for PostgreSQL offre una piattaforma scalabile e altamente disponibile per il database relazionale, garantendo allo stesso tempo la sicurezza e la conformità necessarie per il trattamento dei dati personali.

- Amazon Relational Database Services (RDS) con engine MySQL

Questa risorsa, ospita il Database della componente "Access Point" ed è impiegata nell'ambito del processo descritto al paragrafo 2.4.3.

RDS per MySQL offre un servizio di database relazionale robusto e scalabile, con

funzionalità di sicurezza integrate per la protezione dei dati personali.

- Amazon S3 (Simple Storage Service):

Questo servizio è utilizzato per l'archiviazione dei dati descritti al paragrafo 2.3. Amazon S3 fornisce una soluzione di storage sicura, resiliente e altamente scalabile, con sofisticate funzionalità di controllo dell'accesso per garantire la sicurezza dei dati personali.

In aggiunta a queste risorse è importante sottolineare che, durante la comunicazione tra le varie componenti che compongono l’architettura, i dati personali sono sempre trasmessi in maniera sicura, incapsulati in sessioni HTTPS. Questo garantisce l'integrità e la riservatezza dei dati durante il loro transito.

# II. Principi fondamentali

## 1. Rispetto dei principi di cui all'art. 5 del GDPR

### 1.1. Liceità, correttezza e trasparenza

Il trattamento dei dati personali a mezzo di SDG è effettuato ai sensi dell'art. 6, par. 1, lett. e) del GDPR, per l'esecuzione di un compito di interesse pubblico di cui è investita AGID, seppur in qualità di responsabile del trattamento poiché individuata quale soggetto attuatore e gestore delle componenti italiane di SDG, ai sensi della normativa sopra richiamata.

Il trattamento dei dati personali interviene nel rispetto di quanto previsto dalla regolamentazione unionale e dalle specifiche tecniche delineate dalla Commissione e dagli Stati membri.

La trasparenza del trattamento sarà garantita dall'apposita informativa sul trattamento dei dati personali, resa in merito al funzionamento delle componenti italiane di SDG al fine garantire un agevole e puntuale riferimento – anche mediante rinvio – alle Autorità competenti in qualità di titolari del trattamento.

### 1.2 Limitazione della finalità

I dati personali sono raccolti per finalità determinate, esplicite e legittime – come indicate al paragrafo 1.2. della Parte I della presente analisi - e successivamente trattati in stretta aderenza a tali finalità.

### 1.3. Minimizzazione

I dati personali trattati sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità del trattamento. Durante il periodo di primo avvio di SDG da ottobre a dicembre 2023 con riferimento al solo backoffice del Catalogo dei servizi, ci si riserva in ogni caso di procedere a una rivalutazione della minimizzazione dei dati richiesti, alla luce delle prossime eventuali indicazioni della Commissione e anche a seguito delle interlocuzioni con il RPD e il Garante per la protezione dei dati personali.

### 1.4. Esattezza e aggiornamento

AgID, come soggetto attuatore, limita il proprio intervento all'implementazione e alla

gestione dell'infrastruttura, lasciando in capo alla singola amministrazione in qualità di Autorità competente (specialmente con riferimento alle Autorità che forniscono le prove) la valutazione in merito all'esattezza del dato.

### 1.5. Limitazione della conservazione

I dati personali sono conservati - come indicato nello specifico nella tabella al precedente paragrafo I.3.3. - per l'arco di tempo individuato in base alle necessità legate alle finalità del trattamento, sia in fase di gestione dei dati personali contenuti nelle prove che passano per il nodo, sia in fase di autenticazione degli utenti e dei referenti.

### 1.6. Integrità e riservatezza

L'integrità e la riservatezza dei dati sono perseguite mediante l'adozione delle misure tecniche e organizzative dettagliate nel successivo Capitolo 2, poste in atto al fine di garantire la maggior sicurezza possibile e la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

### 1.7. Responsabilizzazione

AGID, in qualità di responsabile del trattamento, assicura il rispetto effettivo dei principi applicabili al trattamento dei dati personali e opera in modo da poterne rendere conto.
Non appena entrerà in funzione lo sportello digitale unico, AGID inserirà immediatamente le attività di trattamento legate ad esso all'interno del proprio Registro delle attività di trattamento e manterrà un dialogo stretto sia con i titolari del trattamento sia con i sub-responsabili.
In occasione di qualsiasi mutamento delle modalità tecniche o organizzative di gestione dello stesso, la presente analisi del rischio sulla protezione dei dati personali sarà immediatamente rinnovata, al fine di verificare e valutare correttamente i rischi che il trattamento presenta.

## 2. Misure a tutela dei diritti degli interessati

### 2.1. Informativa sul trattamento dei dati personali

Sarà garantita un'apposita informativa sul trattamento dei dati personali, resa in merito al funzionamento delle componenti italiane di SDG al fine garantire un agevole e puntuale riferimento – anche mediante rinvio – alle Autorità competenti in qualità di titolari del

trattamento.

### 2.2. Esercizio dei diritti degli interessati

Gli interessati potranno esercitare i propri diritti contattando le Autorità competenti. AgID resta a piena disponibilità di tutti i titolari per il supporto nel riscontro delle richieste di esercizio dei diritti degli interessati, con riferimento alle attività di competenza.

### 2.3. Trasferimento di dati a Paesi terzi o a organizzazioni internazionali

Non è contemplato nessun trasferimento in Paesi non appartenenti all'Unione Europea o a organizzazioni internazionali al di fuori delle garanzie individuate dalla recente Decisione della Commissione europea del 10 luglio u.s.

### 2.4. Obblighi del responsabile del trattamento

Ai sensi della normativa unionale e nazionale in materia di protezione dei dati personali e, in particolare, dell'art. 28, par. 3, lett. e) del GDPR, AGID quale responsabile del trattamento assisterà le Autorità competenti mediante la predisposizione di adeguate misure tecniche e organizzative per dar seguito alle richieste di esercizio dei diritti dell'interessato.

Le responsabilità di AGID sono previste all'interno dello specifico atto di nomina, sottoscritto da ogni titolare del trattamento ai sensi dell'art. 28 del GDPR.

# III. Rischi

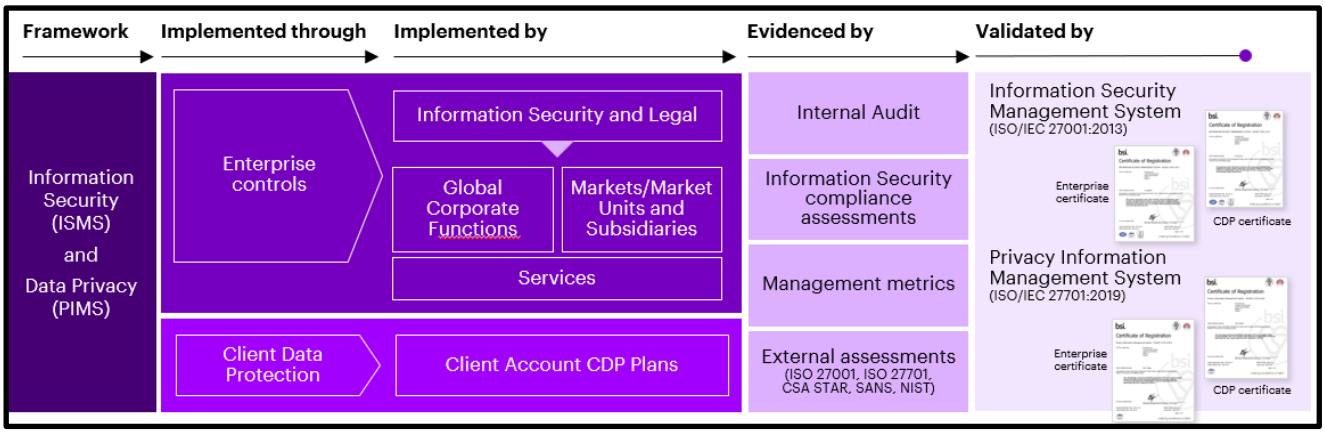
Il Capitolo intende illustrare le misure esistenti o previste per SDG nonché una valutazione qualitativa dei rischi esistenti, sulla base delle minacce e delle misure previste.

## 1. Misure esistenti o pianificate

Per il nodo italiano SDG AgID adotta un sistema di controlli basati sull'utilizzo dei framework ISO 27001 e ISO 27701.

### 1.1. Misure organizzative

Fra le misure organizzative esistenti rientra il sistema di gestione di Information Security (IS) e Data Protection (DP), che si basa sull'utilizzo di una metodologia standardizzata di conformità per la gestione della data privacy e information security (IS) e viene attuato attraverso una serie di processi, controlli e metriche. I sistemi di gestione delle informazioni sulla sicurezza e sulla privacy condividono controlli complementari sulla sicurezza e sulla privacy dei dati. Il programma utilizzato supporta i programmi di certificazione ISO/IEC27001 (IS) e ISO/IEC27701 (DP).




Le componenti principali di tale programma sono:

- Responsabilità: è previsto un responsabile dell'implementazione dei controlli e della gestione della continua conformità afferente all'ambito della valutazione.

- Metodologia di controllo: i controlli IS e DP, basati sulla valutazione del rischio, sono guidati dai dati/servizi degli ambiti progettuali. I controlli sono conformi alle specifiche ISO 27001/27701 per l'archiviazione, l'accesso, la gestione, la trasmissione, l'hosting dei dati.
- Tecnologia IS: le tecnologie di sicurezza hanno come obiettivo il rafforzamento della security posture proteggendo i dati, i server e i dispositivi di rete.
- Formazione e consapevolezza: programma di IS e formazione DP; corsi chiave inclusi nella formazione obbligatoria.
- Requisiti normativi: conformità del piano di IS comune e framework di DP, abbastanza flessibili per affrontare vari scenari.

Utilizzando strumenti di analisi del rischio strutturati, viene determinato un insieme di controlli che riflettono le politiche e gli standard di Information Security e Data Protection.
Di seguito l'ambito dei controlli previsti:

- Access Logging
- Accountability
- Administrator Access
- Approved Devices and Tools
- Change Management
- Cloud
- Content Moderation
- Data Disposal
- Delivery Locations
- Disaster Recovery
- Encryption & Data Storage
- Environment, Config Mgmt.
- Environmental
- Firefighter ID
- Firewall, Antivirus & IDS/IPS
- General Infra. Hosting
- Least Privileged Access
- Legal/Contractual
- Logging & Monitoring
- Managed Security Service
- Movement of People
- Password Management
- Physical Security
- Reuse of Work Products
- Secure Application Dev.
- Incident Reporting
- Subcontractors
- Training
- Transmission of Data
- User Access Management
- Vendor Master Maintenance
- Vulnerability Management

Per quanto riguarda le misure organizzative pianificate, si individuano le revisioni periodiche delle misure organizzative già implementate e dettagliate precedentemente.

### 1.2. Misure tecniche

**A) applicate ai dati:**

- Controllo degli accessi logici tramite AWS IAM e Federazione accessi con IdP qualificati (SPID, CIE, eIDAS). Gli accessi del personale AGID e Fornitori avviane tramite lidentity e Access Management (AWS IAM) che è il servizio che permette di centralizzare il ciclo di vita delle identità digitali che accedono alle risorse AWS verificando che chi è autenticato disponga delle autorizzazioni per utilizzare le risorse della piattaforma. Gli accessi del cittadino sono autorizzati tramite federazione attraverso SPID, CIE, EIDAS mediante la tecnologia AWS Cognito e open source SATOSA. L'accesso al backoffice del catalogo dei servizi nazionale avviene tramite federazione attraverso SPID, CIE, eIDAS mediante la tecnologia AWS Cognito e open source SATOSA.

- La tracciabilità degli accessi ai dati è garantita dal tool nativo AWS Cloud Trail, una piattaforma di Audit Logging che registra e monitora le azioni di accesso eseguite da un utente all'interno dell'infrastruttura SDG. Le azioni di accesso vengono registrate in CloudTrail sotto forma di eventi.

- L'archiviazione dei dati è presente solo all'interno dei database MYSQL dell'applicativo Access Point Domibus protetti da WAF e crittografia at rest.

- Le misure contro i malware sono implementate tramite AWS GuardDuty, strumento di threat analysis; il tool analizza ed elabora i dati dei log forniti dai flow logs, dagli event logs di AWS CloudTrail e dai log DNS per identificare eventuali anomalie rispetto ai setting definiti.

- La crittografia dei dati at rest e in transit è garantita secondo gli standard di settore. La cifratura dei dati at-rest avviene utilizzando protocolli di crittografia simmetrici AES-256. La protezione dei dati in transit è implementata mediante l'utilizzo di modalità di encryption TLS (HTTPS) gestite dal tool Amazon Certificate Manager.

- Il backup e la continuità operativasono assicurati attraverso la funzionalità “automated backup” offerta dal servizio Amazon RDS.

- Il backup dei database viene effettuato con cadenza giornaliera con una retention di 7 giorni.

**B) applicate ai sistemi:**

- Il controllo degli accessi logici avviene tramite AWS IAM e federazione con IdP (SPID, CIE, eIDAS). L’identity e Access Management (AWS IAM) è un servizio che permette di controllare e mantenere sicuri gli accessi alle risorse verificando che chi è autenticato disponga delle autorizzazioni per utilizzare le risorse della piattaforma. Gli accessi dell’utente sono autorizzati tramite federazione attraverso SPID, CIE, eIDAS mediante la tecnologia AWS Cognito e open source SATOSA. L’accesso al backoffice del catalogo dei servizi nazionale avviene tramite federazione attraverso SPID, CIE, eIDAS mediante la tecnologia AWS Cognito e open source SATOSA.

- Le vulnerabilità sono verificate tramite test periodici di SAST, DAST, VA e PT. Gli applicativi e i sistemi sono periodicamente sottoposti a specifici security test relativi agli applicativi e alle infrastrutture che li ospitano.

- Nel contesto Cloud AWS di AgID SDG, il controllo degli accessi fisici è delegato al CSP AWS sulla base dello Shared Responsability Model.

- L’infrastructure security è posta a protezione dell’infrastruttura tramite segmentazione di rete, segregazione degli ambienti, API Gateway, servizi antiDDoS, threat analysis (AWS GuardDuty), Network Access List (NACL) e Security Groups (SG).

- La sicurezza delle interfacce web è garantita tramite AWS WAF. Nel contesto Cloud AWS di AgID SDG viene utilizzata la soluzione WAF nativa di AWS a protezione delle componenti esposte API Gateway, Cloud Front e Load Balancer.

- Il backup e la continuità operativa sono garantiti tramite AWS Backup. Tale

funzionalità, effettua il backup quattro volte al giorno con una retention di 7 giorni su tutte le istanze EC2 delle componenti Access Point e Satosa.

### 1.3. Accesso illegittimo ai dati

- I principali impatti sugli interessati, se il rischio si dovesse concretizzare, potrebbero essere:
    - appropriazione indebita di informazioni e/o documenti
    - sostituzione di persona
    - danno reputazionale
    - social engineering
- le principali minacce che potrebbero concretizzare il rischio potrebbero essere:
    - bug applicativo
    - bug di processo
    - bug di sistema
    - intervento umano
    - furto di credenziali
    - vulnerabilità applicative o infrastrutturali
- le principali fonti di rischio potrebbero essere:
    - malfunzionamenti del software
    - uso improprio di credenziali
    - uso di credenziali rubate
    - interventi umani non corretti
    - non adeguato patching dei sistemi
    - mancate verifiche periodiche di sicurezza
- le misure individuate che contribuiscono a mitigare il rischio sono:
    - Controllo degli accessi logici
    - Tracciabilità
    - Gestione delle Vulnerabilità
    - Contrasto al malware
    - Minimizzazione dei dati
    - Monitoraggio degli Eventi di Sicurezza;
    - Gestione degli incidenti di sicurezza e delle violazioni dei dati personali

Sulla base degli elementi di sopra elencati, l’analisi del rischio, alla luce degli impatti

potenziali e delle misure pianificate risulta: LIMITATA, poiché sono state adottate precauzioni e soluzioni tecniche e si prevedono di attuare ulteriori misure in grado di limitare il rischio.

### 1.4. Modifiche indesiderate dei dati

- I principali impatti sugli interessati, se il rischio si dovesse concretizzare, potrebbero evidenziarsi in:
    - mancata ricezione della documentazione e/o delle informazioni richieste
    - appropriazione di informazioni da parte di terzi
    - social engineering
    - danno reputazionale
    - danno nei rapporti con le P.A.
- Le principali minacce che potrebbero consentire la concretizzazione del rischio possono essere:
    - intervento umano errato
    - bug applicativo
    - bug di sistema
    - bug di processo
    - vulnerabilità applicative o tecnologiche;

- le possibili fonti di rischio possono essere:
    - uso improprio di credenziali
    - utenti che possano operare non correttamente
    - non adeguata conoscenza dei rischi
    - malfunzionamenti del software
    - uso di credenziali rubate
- Le misure, fra quelle individuate, che contribuiscono a mitigare il rischio sono:
    - Controllo degli accessi logici
    - Controllo degli accessi fisici (in carico al CSP)
    - Tracciabilità
    - Minimizzazione dei dati
    - Gestione della vulnerabilità
    - Contrasto al malware
    - Sicurezza dei siti web

- Gestione del personale
- Archiviazione
- Sicurezza dell'hardware (in carico al CSP)
- Gestione degli incidenti di sicurezza e delle violazioni dei dati personali
- Backup
- Gestione delle politiche di continuità operativa

Sulla base degli elementi di sopra elencati, l'analisi del rischio, alla luce degli impatti potenziali e delle misure pianificate risulta: LIMITATA, poiché sono state implementate procedure rigorose di controllo degli accessi, backup regolari e procedure di ripristino in caso di modifiche indesiderate ai dati, riducendo in grado di ridurre al minimo la probabilità di perdita o danneggiamento significativo dei dati.

### 1.5. Perdita dei dati

- I principali impatti sugli interessati, se il rischio si dovesse concretizzare, potrebbero essere:
  - mancata ricezione della documentazione e/o delle informazioni richieste
  - appropriazione di informazioni di terzi
  - danno nei rapporti con la P.A.
  - danno reputazionale
- Le principali minacce che potrebbero consentire la concretizzazione del rischio possono essere:
  - bug applicativo
  - bug di processo
  - bug di sistema
- le possibili fonti di rischio possono essere:
  - malfunzionamento del software
  - operazioni improprie eseguite dal personale
  - attacchi esterni
  - uso di credenziali rubate
- Le misure, fra quelle individuate, che contribuiscono a mitigare il rischio sono:
  - Controllo degli accessi logici
  - Controllo degli accessi fisici (in carico al CSP)
  - Tracciabilità degli eventi
  - Archiviazione dei dati e degli eventi

- Gestione delle vulnerabilità
- Contrasto al malware
- Sicurezza dei siti web
- Backup
- Gestione delle politiche di continuità operativa
- Prevenzione delle fonti di rischio
- Prevenzione e gestione degli incidenti di sicurezza e delle violazioni dei dati personali

Sulla base degli elementi di sopra elencati, l'analisi del rischio, alla luce degli impatti potenziali e delle misure pianificate risulta: LIMITATA, poiché sono state adottate precauzioni e soluzioni tecniche quali procedure di backup, crittografia dei dati e controlli di sicurezza per garantire la protezione dei dati e prevenire la loro perdita. Inoltre, sono condotti regolarmente test di sicurezza per assicurare che tali misure siano efficaci nel mitigare il rischio di perdita dei dati.

### 1.6. Panoramica dei rischi

Con le misure di sicurezza organizzative e tecniche pianificate, la panoramica dei rischi, come sopra dettagliata, risulta pertanto la seguente:

| Casistica | Gravità del rischio | Probabilità del rischio |
|---|---|---|
| **Accesso illegittimo ai dati** | *LIMITATA* | *LIMITATA* |
| **Modifiche indesiderate ai dati** | *LIMITATA* | *LIMITATA* |
| **Perdita dei dati** | *LIMITATA* | *LIMITATA* |

# IV. Convalida

## 1. Piano d'azione

| Parte I - Contesto | |
|---|---|
| Cap. 1 - Panoramica del trattamento | Revisione periodica, con primo termine entro dicembre 2023 |
| Cap. 2 - Dati, processi e risorse a supporto | Revisione periodica, con primo termine entro dicembre 2023 |
| **Parte II - Principi fondamentali** | |
| Cap. 1 - Rispetto dei principi di cui all'art. 5 GDPR | Revisione periodica, con primo termine entro dicembre 2023 |
| Cap. 2 – Misure a tutela dell'interessato | Revisione periodica, con primo termine entro dicembre 2023 |
| **Parte III - Rischi** | |
| Cap. 1 – Misure esistenti o pianificate | Revisione periodica, con primo termine entro dicembre 2023 |

Si specifica che la presente analisi del rischio sulla protezione dei dati personali e la conseguente decisione in merito all'attivazione di specifici piani di azione saranno periodicamente rivalutate e aggiornate alla luce dell'evoluzione ancora in corso delle specifiche tecniche e di protezione dei dati e dell'interlocuzione con il Garante per la protezione dei dati personali.

## 2. Parere del R.P.D.

Si allega alla presente il parere reso dal RPD sul presente documento, a valle dell'analisi svolta unitamente al Servizio di riferimento.

## 3. Convalida

La presente analisi del rischio sulla protezione dei dati personali, effettuata ai sensi della normativa unionale e nazionale in materia, è sottoscritta digitalmente dal Direttore generale Ing. Mario Nobile ai fini della relativa convalida.

**Il Direttore Generale**

**Ing. Mario Nobile**

*Firmato Digitalmente da/Signed by:*
**MARIO NOBILE**
*In Data/On Date:*
**lunedì 2 ottobre 2023 19:45:44**