AGID
Agenzia per l'Italia Digitale

Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati

ai sensi dell'articolo 50-ter, comma 2 del D. Lgs. 7 marzo 2005, n. 82

Versione 2.0 del 19 giugno 2025

Versione	Data	Tipologia modifica
1.0	06.12.2021	Prima emissione.

2.0	19.06.2025	- Aggiunti al paragrafo 2.2:
		  - Allegato 4: Processo di distribuzione dei segnali di variazione;
		  - Allegato 5: Scambio di dati/informazioni asincrono con callback;
		  - Allegato 6: Modelli di Collaborazione;
		  - Allegato 7: Regole di popolamento.
		- Modificato paragrafo 3.1.
		- Modificata nel capitolo 4 la definizione di Capofila in Delegato dell'Erogatore
		- Aggiunte in capitolo 4 definizioni:
		  - Finalità;
		  - Delegato;
		  - Erogazione Inversa;
		  - Erogazione Ordinaria;
		  - Richiesta Massiva;
		  - Modalità Asincrona;
		  - Segnale di Variazione;
		  - Produttore;
		  - Consumatore;
		  - Funzione di hashing;
		  - Funzione di hashing con seme;
		  - Identificatore pseudonimizzato.
		- Aggiunto capitolo 5.
		- Modificati capitoli 6, 7, 8, 9, 10, 11, 12 e 13.
		- Aggiunto capitolo 14.
		- Modificato capitolo 15.
		- Aggiunti capitoli 16 e 17.
		- Modificato capitolo 18.

Indice

1. Introduzione

Nell'ambito del modello di interoperabilità delle pubbliche amministrazioni (di seguito **MoDI**), le presenti **Linee Guida** (di seguito **Linee Guida**) concernono la Piattaforma Digitale Nazionale Dati (di seguito **PDND**) di cui all'articolo 50-ter del decreto legislativo 7 marzo 2005, n. 82 e s.m.i. recante il "Codice dell'amministrazione digitale" (di seguito **CAD**), avendo ad oggetto l'infrastruttura tecnologica per l'interoperabilità dei sistemi informativi e delle basi di dati (di seguito **Infrastruttura interoperabilità PDND**) di cui al comma 2 del medesimo articolo.

Ai sensi dell'articolo 50-ter, comma 1 del **CAD**, la **PDND** è finalizzata a favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto per finalità istituzionali dai soggetti di cui all'articolo 2, comma 2 del **CAD** nonché la condivisione dei dati/informazioni tra i soggetti che hanno diritto di accedervi ai fini dell'attuazione dell'articolo 50 del **CAD** e della semplificazione degli adempimenti dei cittadini e delle imprese, in conformità alla normativa vigente.

Ai sensi dell'articolo 50-ter, comma 2 del **CAD**, l'**Infrastruttura interoperabilità PDND** rende possibile l'interoperabilità dei sistemi informativi e delle basi di dati dei soggetti interessati, mediante:

- l'accreditamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati a operare sulla stessa;
- la raccolta e la conservazione delle informazioni relative agli accessi e alle transazioni effettuati suo tramite.

Ai sensi dell'art. 50-ter, comma 2-bis, del **CAD**, il Presidente del Consiglio dei ministri o il Ministro delegato per l'innovazione tecnologica e la transizione digitale, ultimati i test e le prove tecniche di corretto funzionamento della **Infrastruttura interoperabilità PDND**, fissa il termine entro il quale i soggetti di cui all'articolo 2, comma 2, del **CAD** saranno tenuti ad accreditarsi alla stessa, a sviluppare le interfacce e a rendere disponibili le proprie basi dati.

I soggetti di cui all'articolo 2, comma 2, del **CAD DEVONO** aderire e utilizzare l'**Infrastruttura interoperabilità PDND** per tutte le API da essi realizzate e utilizzate, nei termini e con le modalità previsti dall'articolo 50-ter del **CAD**.

Le **Linee Guida** sono emanate ai sensi dell'articolo 50-ter, comma 2, ultimo periodo del **CAD**, che dispone quanto segue: *"L'AgID, sentito il Garante per la protezione dei dati personali e acquisito il parere della Conferenza unificata, di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta linee guida con cui definisce gli standard tecnologici e criteri di sicurezza, di accessibilità, di disponibilità e di interoperabilità per la gestione della piattaforma nonché il Processo di adesione e di fruizione del catalogo API con i limiti e le condizioni di accesso volti ad assicurare il corretto trattamento dei dati personali ai sensi della normativa vigente"*.

Più in particolare, le **Linee Guida** individuano:

- i processi di accreditamento, identificazione e autorizzazione assicurati dalla **Infrastruttura interoperabilità PDND**;
- le modalità con cui i soggetti interessati danno seguito alle reciproche transazioni per il tramite dell'**Infrastruttura interoperabilità PDND**;
- le modalità di raccolta e conservazione delle informazioni relative agli accessi e alle transazioni effettuate mediante l'**Infrastruttura interoperabilità PDND**.

Si chiarisce che presenti **Linee Guida** sono redatte a valle dell'ultima modifica normativa intervenuta sul testo dell'art. 50, comma 2-ter del **CAD**, la quale ha previsto l'eliminazione degli accordi quadro attraverso cui le pubbliche amministrazioni assicuravano la fruizione dei dati in proprio possesso alle altre pubbliche amministrazioni e ai gestori di servizi pubblici.

2. Riferimenti e sigle

2.1. Note di lettura del documento

Conformemente alle norme *ISO/IEC Directives, Part* per la stesura dei documenti tecnici, le presenti **Linee Guida** utilizzeranno le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «DOVREBBE», «NON DOVREBBE», «PUÒ», «POSSONO» e «OPZIONALE», la cui interpretazione è descritta di seguito.

- **DEVE** o **DEVONO**, indicano un requisito obbligatorio per rispettare la linea guida;
- **NON DEVE** o **NON DEVONO** o **NON PUÒ** o **NON POSSONO**, indicano un assoluto divieto delle specifiche;
- **DOVREBBE** o **NON DOVREBBE**, indicano che le implicazioni devono essere comprese e attentamente pesate prima di scegliere approcci alternativi;
- **PUÒ** o **POSSONO** o l'aggettivo **OPZIONALE**, indica che il lettore può scegliere di applicare o meno senza alcun tipo di implicazione la specifica.

2.2. Struttura

Considerata la velocità dell'innovazione, le **Linee Guida** devono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Di qui la scelta di allegare alle presenti **Linee Guida** alcuni documenti i cui contenuti potranno essere adeguati più agevolmente all'evoluzione tecnologica. Tale processo di costante adeguamento degli allegati è realizzato in coerenza con il quadro normativo in materia di digitalizzazione e, nello specifico, ai sensi dell'articolo 14-bis, comma 2, lettera a) del **CAD**, che assegna ad AgID la funzione di "emanazione di **Linee Guida** contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea".

Le presenti **Linee Guida** includono i seguenti allegati:

- Allegato 1: Processo di adesione e Accordo di Adesione
- Allegato 2: Pubblicazione e fruizione delle API
- Allegato 3: Standard e dettagli tecnici utilizzati per la fruizione dei Voucher di autorizzazione
- Allegato 4: Processo di distribuzione dei segnali di variazione
- Allegato 5: Scambio di dati/informazioni asincrono con callback
- Allegato 6: Modelli di Collaborazione
- Allegato 7: Regole di popolamento

2.3. Riferimenti normativi

Sono riportati di seguito gli atti normativi di principale riferimento per le presenti **Linee Guida**.

[CAD]	Decreto legislativo 7 marzo 2005, n. 82 e s.m.i. recante "Codice dell'amministrazione digitale".
[D.L. 135/2018]	Decreto-legge 14 dicembre 2018, n. 135 recante "Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione",

	convertito in Legge, con modificazioni, dall'art. 1, comma 1 della Legge 11 febbraio 2019, n. 12.
[GDPR]	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
[eIDAS]	Regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
[Codice privacy]	Decreto legislativo 30 giugno 2003, n. 196 e s.m.i. recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE".
[Decreto 22/09/2022]	Decreto 22 settembre 2022 recante "Obblighi e termini di accreditamento alla Piattaforma Digitale Nazionale Dati".
[Decreto 05/12/2023]	Decreto 5 dicembre 2023 recante "Misure per l'attuazione dell'articolo 50-ter del decreto legislativo 7 marzo 2005, n. 82".

2.4. Linee Guida di primario riferimento

Di seguito sono elencate le linee guida emesse dall'AgID che verranno espressamente richiamate nelle presenti **Linee Guida**.

[LG INTEROPERABILITÀ TECNICA]	Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni
[LG SICUREZZA]	Linee Guida Tecnologie e standard per assicurare la sicurezza dell'interoperabilità tramite API dei sistemi informatici

2.5. Acronimi

Di seguito si riportano gli acronimi utilizzati nelle presenti **Linee Guida**.

[MoDI]	Modello di Interoperabilità della Pubblica Amministrazione, definito dalle Linee Guida emanate in materia da AgID ai sensi dell'articolo 71 del CAD
[QoS]	Quality of Service, ovvero l'indicazione dei parametri usati per caratterizzare la qualità degli e-service
[SLA]	Service Level Agreement, ovvero accordo sul livello di servizio frutto della contrattazione tra erogatore e fruitore
[SLI]	Service-Level Indicator, ovvero metrica atta a misurare l'efficienza dei servizi individuati dall'erogatore
[SLO]	Service-Level Objective, ovvero gli obiettivi degli SLI per i servizi definiti dall'erogatore

3. Ambito di applicazione

Le presenti **Linee Guida** sono emanate ai sensi dell'articolo 71 del **CAD** e della Determinazione dell'Agenzia per l'Italia Digitale (di seguito AgID) n. 160 del 17 maggio 2018 recante *"Regolamento per l'adozione di linee guida per l'attuazione del Codice dell'Amministrazione Digitale"*.

3.1. Soggetti destinatari

3.1.1. Soggetti erogatori

Le presenti **Linee Guida** sono destinate ai soggetti di cui all'articolo 2, comma 2, del **CAD** e nonché ai privati che, nello svolgimento di attività connesse al perseguimento di finalità di interesse pubblico, hanno l'esigenza di condividere i propri dati con i soggetti fruitori di cui al paragrafo 3.1.2, alle condizioni fissate dall'ordinamento. Tali soggetti sono abilitati ad erogare tramite la PDND i loro dati, agendo in qualità di **soggetti erogatori**.

I **soggetti erogatori** per il tramite della **Infrastruttura interoperabilità PDND**, favoriscono:

- la conoscenza e l'utilizzo del patrimonio informativo detenuto per finalità istituzionali nelle banche dati a loro riferibili,
- la condivisione dei dati/informazioni con i soggetti che hanno diritto di accedervi in attuazione dell'articolo 50 del **CAD** per la semplificazione degli adempimenti dei cittadini e delle imprese,
- l'integrazione di processi funzionali alla semplificazione degli adempimenti dei cittadini e delle imprese,

assicurando le modalità di scambio telematico per il tramite di API, come previsto dal **MoDI**.

In particolare, i **soggetti erogatori** attuano le **Linee Guida** al fine di condividere i dati/informazioni da essi detenuti e l'integrazione di processi, assicurando:

- l'implementazione di interfacce di programmazione delle applicazioni accessibili tramite Internet (di seguito API) conformi alle [LG INTEROPERABILITÀ TECNICA];
- la registrazione delle API, di cui al precedente punto, nel **Catalogo API** reso disponibile dell'**Infrastruttura interoperabilità PDND**.

3.1.2. Soggetti fruitori

Le **Linee Guida** sono rivolte, altresì, ai soggetti di cui all'articolo 2, comma 2, del **CAD** nonché ai privati che nello svolgimento delle proprie attività, ai sensi dell'art. 50-ter del CAD, hanno l'esigenza di fruire e riutilizzare i dati dei soggetti erogatori di cui al paragrafo 3.1.1, alle condizioni fissate dall'ordinamento. Tali soggetti sono abilitati a fruire della **PDND** al fine di accedere ai dati e alle informazioni ivi resi disponibili ed agiscono in qualità di **soggetti fruitori**.

Resta fermo quanto chiarito all'art. 50, comma 3-ter del **CAD**: *"Il trasferimento di un dato da un sistema informativo a un altro non modifica la titolarità del dato e del trattamento, ferme restando le responsabilità delle amministrazioni che ricevono e trattano il dato in qualità di titolari autonomi del trattamento"*.

3.1.3. Gestore

Le **Linee Guida**, infine, sono rivolte altresì al gestore dell'**Infrastruttura interoperabilità PDND** (di seguito **Gestore**), come individuato ai sensi dell'art. 50-ter del **CAD**, il quale le attua in merito alla progettazione, allo sviluppo e alla gestione dell'infrastruttura.

4. Definizioni

4.1. Aderente

È il soggetto che aderisce alla **Infrastruttura interoperabilità PDND** attraverso il Processo di adesione (si veda Capitolo 6 Adesione) per erogare e/o fruire di servizi mediante le funzionalità dell'infrastruttura rispettivamente nella funzione di **soggetto erogatore**, di cui al paragrafo 3.1.1, e di **soggetto fruitore**, di cui al paragrafo 3.1.2.

4.2. Accordo di Adesione

È il documento sottoscritto dall'Aderente (personalmente o mediante il proprio legale rappresentante in caso di soggetto giuridico) al fine di aderire alla **Infrastruttura interoperabilità PDND** e utilizzare le funzionalità ivi messe a disposizione.

4.3. Erogatore

È un **Aderente** che rende disponibili **e-service** ad altri **Aderenti** mediante le funzionalità della **Infrastruttura Interoperabilità PDND**, per la fruizione di dati/informazioni conservate in un archivio, tenuto sotto la propria responsabilità e che è considerato una fonte primaria di tali dati/informazioni, per la ricezione di dati/informazioni da parte di un altro **Aderente**, o per l'integrazione di processi.

4.4. Finalità

Con Finalità si indica la ragione per cui un **Fruitore** intende accedere ad un **e-service**.

4.5. Fruitore

È un **Aderente** che fruisce degli **e-service** messi a disposizione da un **Erogatore** mediante le funzionalità della **Infrastruttura Interoperabilità PDND**.

4.6. Attributi degli Aderenti

Sono le caratteristiche dell'Aderente, disciplinate nel Capitolo 7 Gestione degli Attributi degli Aderenti.

4.7. Registro degli Attributi

È la sezione dell'**Infrastruttura interoperabilità PDND** in cui sono raccolti, a cura del **Gestore**, gli **Attributi degli Aderenti** che POSSONO essere utilizzati dagli **Erogatori** per la definizione dei **Requisiti di Fruizione** dei propri **e-service**.

4.8. Utenti degli Aderenti

Sono gli utenti registrati dagli **Aderenti** sull'**Infrastruttura interoperabilità PDND** e delegati all'uso e alla gestione delle funzionalità ivi rese disponibili.

Le funzionalità rese disponibili dall'**Infrastruttura interoperabilità PDND** agli **Utenti degli Aderenti** e i ruoli che questi possono ricoprire sono riportati nell'ALLEGATO 2: PUBBLICAZIONE E FRUIZIONE DELLE API.

4.9. Delegato

L'**Infrastruttura interoperabilità PDND** promuove la collaborazione tra pubbliche amministrazioni di cui all'articolo 2, comma 2, lettera a), del **CAD** tramite il ruolo del **Delegato**.

Il **Delegato** è una pubblica amministrazione di cui all'articolo 2, comma 2, lettera a), del **CAD**, **Aderente** all'**Infrastruttura interoperabilità PDND**, che è delegata da un'altra pubblica amministrazione **Aderente** a utilizzare per suo conto le funzionalità dell'infrastruttura medesima per:

- la registrazione e la modifica degli **e-service** sul **Catalogo API**, ivi compresa l'accettazione delle richieste di fruizione per gli stessi (**Delegato dell'Erogatore**);
- la compilazione e la sottoposizione delle richieste di fruizione degli **e-service** di interesse, ivi compresa la compilazione delle analisi del rischio (**Delegato del Fruitore**).

Una pubblica amministrazione **Aderente PUÒ** candidarsi ad assumere il ruolo di **Delegato** registrando tale volontà sull'**Infrastruttura interoperabilità PDND**.

Le pubbliche amministrazioni **Aderenti POSSONO** delegare uno o più **Delegati** tra quelli che si sono candidati a tale fine sull'**Infrastruttura interoperabilità PDND** ma non può delegare più **Delegati** per l'erogazione o la fruizione di uno stesso **e-service**.

La delega al **Delegato** ha effetto al momento dell'accettazione di quest'ultimo e determina la possibilità, per i suoi Utenti, di operare sull'**Infrastruttura interoperabilità PDND** per conto dell'**Aderente** delegante.

4.10. API

Un insieme di procedure, funzionalità e/o operazioni disponibili al programmatore, di solito raggruppate a formare un insieme di strumenti specifici per l'espletamento di un determinato compito.

4.11. Template e-service

Per Template e-service si intende un modello di descrittore di un **e-service** in cui restano liberi alcuni elementi operativi necessari alla reale operatività dell'e-service. In tal modo il Template e-service resta un modello astratto di riferimento, a cui gli **Aderenti** POSSONO attenersi durante il processo di implementazione.

4.12. e-service

Nelle presenti **Linee Guida** si applica la definizione di **e-service** presente nelle [LG INTEROPERABILITÀ TECNICA].

In breve, si tratta di un servizio digitale realizzato da un **Erogatore**, attraverso l'implementazione delle necessarie API conformi alle [LG INTEROPERABILITÀ TECNICA] e alle [LG SICUREZZA], per assicurare ai **Fruitori** l'accesso ai propri dati/informazioni e/o l'integrazione coi propri processi. Gli **e-service** POSSONO anche consentire ad un **Fruitore** di comunicare dati/informazioni di sua titolarità all'Erogatore.

4.13. Erogazione Inversa

Per **Erogazione Inversa** si intende il flusso descritto per l'accesso ad un **e-service** che consente ad un **Erogatore** la ricezione di dati/informazioni di cui un **Fruitore** è titolare.

4.14. Erogazione Ordinaria

Per **Erogazione Ordinaria** si intende il flusso descritto per l'accesso ad un **e-service** che consente ad un **Fruitore** di accedere ai dati/informazioni di cui l'Erogatore è titolare.

4.15. Catalogo API

Il **Catalogo API,** anche nominato **Catalogo degli e-service,** costituisce la componente unica e centralizzata prevista dalle [LG INTEROPERABILITÀ TECNICA] che assicura agli **Erogatori** la registrazione e la pubblicazione dei propri **e-service** e ai **Fruitori** la consultazione degli **e-service** pubblicati.

Il **Catalogo API** è realizzato dall'**Infrastruttura interoperabilità PDND**.

4.16. Requisiti di Fruizione

Associati da ogni **Erogatore** a ciascun **e-service** pubblicato sul **Catalogo API**, indicano gli **Attributi degli Aderenti** che un **Fruitore** deve possedere per poter fruire dell'e-service.

Gli **Erogatori** utilizzano gli **Attributi degli Aderenti** presenti nel **Registro degli Attributi** per definire i **Requisiti di Fruizione** degli **e-service**.

4.17. Voucher

È la rappresentazione digitale degli elementi utili ad applicare i **Requisiti di Fruizione** richiesti per l'accesso a ogni **e-service** ed è rilasciato dall'**Infrastruttura interoperabilità PDND** in relazione a ogni richiesta di fruizione di un **e-service**.

Il **Fruitore** presenta all'**Erogatore** il **Voucher** rilasciato dall'**Infrastruttura interoperabilità PDND** e quest'ultimo lo utilizza per verificare il soddisfacimento dei **Requisiti di Fruizione** per l'accesso all'e-service.

4.18. Pattern di interazione

Individuati nelle [LG INTEROPERABILITÀ TECNICA], indicano le modalità tecniche per implementare i modelli di scambio telematico tra **Erogatori** e **Fruitori** tramite API.

4.19. Pattern di sicurezza

Individuati nelle [LG INTEROPERABILITÀ TECNICA] nel rispetto delle [LG SICUREZZA], delineano le modalità tecniche per assicurare che i Pattern di interazione rispettino specifiche esigenze di sicurezza (autenticazione e autorizzazione delle parti, confidenzialità delle comunicazioni, integrità dei messaggi scambiati, ecc.).

4.20. Profili di interoperabilità

Individuati nelle [LG INTEROPERABILITÀ TECNICA], sono combinazioni di Pattern di interazione e Pattern di sicurezza volte a risolvere esigenze di interazione specifiche tra **Erogatori** e **Fruitori** tramite API.

4.21. Service Level Agreements (SLA)

Sono accordi sui livelli di servizio che **Erogatore** e **Fruitore** POSSONO concordare autonomamente, senza il coinvolgimento dell'**Infrastruttura interoperabilità PDND**, con riferimento a un determinato **e-service** al fine di stabilire la relativa QoS (Quality of Service).

Gli SLA concordati fra **Erogatori** e **Fruitori** DEVONO essere coerenti con gli SLA dichiarati dal **Gestore** per l'operatività dell'**Infrastruttura interoperabilità PDND**.

Le eventuali controversie sull'applicazione degli SLA sono risolte autonomamente fra **Erogatore** e **Fruitore**.

4.22. Richiesta Massiva

Modalità asincrona di richiesta massiva di scambio di dati/informazioni tramite la quale un **Fruitore** può aggregare in un'unica chiamata ad un **e-service** interrogazioni omogenee ma relative a identificativi diversi.

4.23. Modalità Asincrona

Modalità di scambio di dati/informazioni attraverso la quale al **Fruitore**, a fronte di una sua richiesta, non viene restituita immediatamente la risposta ma l'**Erogatore** conferma solo la presa in carico della operazione. Il fruitore deve prevedere di ricevere la risposta in un secondo tempo, quando l'erogatore avrà terminato di elaborare l'operazione richiesta.

4.24. Segnale di Variazione

Evento tramite il quale un **Aderente Produttore** comunica **agli Aderenti Consumatori,** per il tramite della **Piattaforma interoperabilità PDND**, l'avvenuta variazione dii stati e/o fatti conosciuti all'interno del dominio di dati/informazioni di cui lo stesso è titolare.

4.25. Produttore

È un **Aderente** che inserisce sulla **Piattaforma interoperabilità PDND** dei segnali di variazione in modo da rendere note le variazioni degli stati e fatti conosciuti all'interno del dominio di dati/informazioni di cui lo stesso è titolare.

4.26. Consumatore

È un **Aderente** che recupera dalla **Piattaforma interoperabilità PDND** i segnali di variazione in modo da essere consapevole delle variazioni degli stati e fatti di sua competenza e interesse.

4.27. Funzione di hashing

Una funzione crittografica di hashing (in breve funzione di hashing) è caratterizzata dalle seguenti proprietà:

- deve essere assicurare l'univocità dell'associazione input/output, ovvero non è possibile che due differenti input, pur essendo simili, abbiano lo stesso valore di hash;
- deve essere deterministica, cioè lo stesso input si traduce sempre nello stesso hash;
- deve essere quasi impossibile generare un input dal suo valore hash se non provando tutti gli input possibili.

4.28. Funzione di hashing con seme

Una funzione di hashing con seme è un tipo di funzione di hashing che richiede in input un valore aggiuntivo chiamato "seme", utilizzato come parametro.

L'aggiunta del seme rende più sicuro il processo di hash in quanto rende più difficile per un potenziale attaccante prevedere o trovare un pattern nei risultati di hashing, migliorando la resistenza ai tentativi di attacco.

4.29. Identificatore pseudonimizzato

Un identificatore pseudonimizzato è un dato ottenuto attraverso l'applicazione di una funzione di hashing su un identificatore originale, rendendo così difficile l'associazione diretta con la persona fisica corrispondente senza l'uso di informazioni aggiuntive.

5. Processo di aggiornamento degli Allegati

Gli Allegati delle **Linee Guida** disciplinano le modalità operative con cui gli **Aderenti**, mediante l'**Infrastruttura interoperabilità PDND**, realizzano l'interoperabilità dei propri sistemi informatici.

Le modalità operative che gli **Aderenti DEVONO** utilizzare sono indicate negli allegati alle presenti L**inee Guida**.

Nel caso in cui un **Aderente** abbia l'esigenza di aggiornare le esistenti modalità operative, e/o di introdurre delle nuove, DEVE segnalare la circostanza ad AgID, definendo un'esigenza e/o formulando una proposta.

AgID, su richiesta di un **Aderente** o su propria iniziativa, avvia un tavolo pubblico di concertazione per modificare o definire nuove modalità operative. Le nuove modalità operative, o la modifica di quelle esistenti, sono formalmente introdotte nelle presenti **Linee Guida** attraverso Circolari emanate da AgID per l'aggiornamento degli allegati.

Gli aggiornamenti indicati NON DEVONO:

- determinare modifiche sulla modalità di trattamento di dati personali, e
- introdurre nuove funzionalità obbligatorie che determinano nuovi oneri agli **Aderenti**.

AgID assicura la possibilità di manifestare l'esigenza e/o formulare una proposta di aggiornamento e/o introduzione delle nuove modalità operative dal 1° gennaio al 31 dicembre di ogni anno.

A tal fine, AgID pianifica annualmente i due seguenti cicli di proposta:

(i) ° ciclo [1° ottobre anno corrente - 30 giugno anno successivo]

- [NUOVA ESIGENZA E PROPOSTA] da 1° ottobre anno corrente - 28 febbraio anno successivo
- [CONCERTAZIONE] dal 1° gennaio anno successivo - 30 aprile anno successivo
- [ADOZIONE] dal 1° maggio anno successivo - 30 giugno anno successivo

(i+1) ° ciclo [1° marzo anno corrente - 31 gennaio anno successivo]

- [NUOVA ESIGENZA E PROPOSTA] da 1° marzo anno corrente - 30 settembre anno corrente
- [CONCERTAZIONE] dal 1° agosto anno corrente - 30 novembre anno corrente
- [ADOZIONE] dal 1° dicembre anno corrente - 31 gennaio anno successivo

Il **Gestore** rende disponibili gli **strumenti per dare seguito ai cicli di proposta** sulla base dei requisiti definiti da AgID.

5.1. Nuova esigenza e proposta

Nel caso in cui un **Aderente** non riesca a soddisfare una propria esigenza tecnica utilizzando le modalità operative disponibili DEVE segnalare la circostanza ad AgID, inviando una comunicazione per il tramite degli **strumenti per dare seguito ai cicli di proposta**. Nella segnalazione ad AgID, l'Aderente PUÒ formulare una proposta di una nuova modalità operativa per l'esigenza segnalata.

AgID, entro 30 giorni dalla ricezione della segnalazione, ove ritenga non sussistano le condizioni per avviare la fase di concertazione, ne dà comunicazione all'Aderente.

5.2. Concertazione e Adozione

AgID, ove ritenga sussistano le condizioni, avvia la fase di concertazione rendendo pubblica le esigenze manifestate dagli **Aderenti**, unitamente alle eventuali proposte formulate, per il tramite degli **strumenti per dare seguito ai cicli di proposta**.

Gli **strumenti per dare seguito ai cicli di proposta** mettono a disposizione un canale di comunicazione tramite cui è possibile presentare proposte di modalità operative che rispondano all'esigenza manifestate dagli **Aderenti** e/o evidenziare eventuali mancanze riscontrate nelle modalità operative proposte.

Nella fase di adozione, AgID, considerando le eventuali proposte ricevute nella fase di concertazione, adotta la/e modalità operativa/e che risponda/no all'esigenze manifestate. Le modalità operative adottate da AgID costituiscono parte integrante e sostanziali delle presenti **Linee Guida** e saranno in queste inserite attraverso le Circolari emanate da AgID per aggiornare gli allegati tecnici.

6. Adesione

I soggetti di cui al paragrafo 3.1 richiedono l'accreditamento sull'**Infrastruttura interoperabilità PDND** mediante il Processo di adesione, che prevede sommariamente i seguenti passaggi:

1. identificazione, tramite una delle modalità previste dall'articolo 64 del **CAD**, del:
    a. soggetto **Aderente**, qualora si tratti di persona fisica;
    b. del rappresentante legale o di un suo delegato, qualora l'**Aderente** sia una persona giuridica;
2. qualificazione del soggetto **Aderente**. Con riferimento gestori di pubblico servizio, si specifica che nel caso in cui si riscontri l'assenza nell'IPA del soggetto richiedente l'adesione, oppure quest'ultimo rilevi la non correttezza del domicilio digitale registrato nell'IPA, il soggetto richiedente l'adesione **DEVE** provvedere all'integrazione e/o correzione dei dati registrati nell'IPA utilizzando le procedure ivi previste, e finché tale integrazione/correzione non avverrà il **Gestore DEVE** considerare tale soggetto come un'impresa di natura privata;
3. invio, da parte della **Infrastruttura interoperabilità PDND** al domicilio digitale dell'**Aderente** della comunicazione recante le informazioni concernenti la richiesta di accreditamento e il codice di controllo necessario ad abilitare la prosecuzione di tale processo;
4. l'**Aderente** recupera dalla **Infrastruttura interoperabilità PDND** l'**Accordo di Adesione**, provvede alla sottoscrizione con firma elettronica ai sensi del Regolamento eIDAS dello stesso **Accordo di Adesione** e al relativo caricamento sulla **Infrastruttura interoperabilità PDND**.

La conclusione del Processo di adesione determina, nel caso in cui l'**Aderente** sia un soggetto giuridico, l'abilitazione del legale rappresentante o di un suo delegato, in qualità di **Utente dell'Aderente**, a utilizzare per conto dell'**Aderente** le funzionalità rese disponibili dall'**Infrastruttura interoperabilità PDND**.

Il Processo di adesione è dettagliatamente disciplinato nell'ALLEGATO 1: PROCESSO DI ADESIONE E ACCORDO DI ADESIONE.

L'adesione alla **Infrastruttura interoperabilità PDND** è condizionata alla sussistenza delle condizioni che l'hanno determinata.

Il **Gestore PUÒ** verificare la qualità di società a controllo pubblico ai sensi dell'art. 2, comma 2, lett. c, del **CAD**, tramite l'autodichiarazione rilasciata in fase di adesione ai sensi del DPR 445/2000.

Il **Gestore DEVE** periodicamente verificare le condizioni che hanno determinato l'adesione dei soggetti interessati.

Il **Gestore:**

- **DEVE** mettere a disposizione degli **Aderenti**:
    - un'istanza dell'**Infrastruttura interoperabilità PDND** di produzione, che gli **Aderenti** utilizzano con dati reali e con valore amministrativo, al fine di permettere l'erogazione e fruizione degli **e-service**;
    - un'istanza dell'**Infrastruttura interoperabilità PDND** di collaudo, che gli **Aderenti** utilizzano con dati fittizi e senza alcun valore amministrativo, al fine di permettere la verifica e lo studio delle interazioni tecnologiche con gli **e-service**;
- **PUÒ** mettere a disposizione degli **Aderenti** e ad altri soggetti un'istanza dell'**Infrastruttura interoperabilità PDND**, che gli stessi utilizzano con dati fittizi e senza alcun valore amministrativo, al fine di permettere la verifica e lo studio delle funzionalità della stessa **Infrastruttura interoperabilità PDND**, nonché delle interazioni tecnologiche con gli **e-service**.

7. Gestione degli attributi degli Aderenti

L'Infrastruttura interoperabilità **PDND** detiene il **Registro degli Attributi**.

Gli **Attributi degli Aderenti** sono necessari a individuare se l'**Aderente**, che fa richiesta di fruizione di un **e-service** in veste di **Fruitore**, possieda i **Requisiti di Fruizione** richiesti dall'Erogatore per quel determinato **e-service**.

Gli **Attributi** possono consistere: in un'affermazione/negazione del possesso di un determinato requisito da parte di un **Aderente** (C.d. "Caso booleano", con risposta "si/no") oppure nell'associazione di un valore alfanumerico ad un **Aderente**.

I **Requisiti di Fruizione** possono, a scelta dell'**Erogatore**, richiedere il mero possesso di un **Attributo** oppure la verifica che il valore associato all'**Attributo** rientri in un determinato insieme di valori.

L'Infrastruttura interoperabilità **PDND** assicura la gestione delle seguenti tipologie di **Attributi degli Aderenti**:

a. **Certificati**: sono gli attributi associabili agli **Aderenti** in maniera automatica dalla **Infrastruttura interoperabilità PDND** limitatamente alle informazioni necessarie:
   - all'adesione alla **Infrastruttura interoperabilità PDND**, mediante l'utilizzo dei dati contenuti nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) di cui all'articolo 6-ter del **CAD**, nell'Indice nazionale delle imprese e dei professionisti (INI-PEC) di cui all'articolo 6-bis del **CAD**, nel Registro delle Imprese di cui alla legge di riordino delle Camere di Commercio (L. 580/1993) e nell'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (INAD) di cui all'articolo 6-quater del **CAD**, come dettagliato e specificato nell' ALLEGATO 1: PROCESSO DI ADESIONE E ACCORDO DI ADESIONE;
   - alla fruizione degli **e-service**, mediante l'utilizzo dei dati contenuti nelle basi di dati di interesse nazionale di cui all'art. 60 del **CAD** o in eventuali altre banche dati di interesse pubblico riferibili ad autorità di vigilanza o controllo, individuate nella valutazione d'impatto sulla protezione dei dati personali a cura del **Gestore**, considerate le specifiche esigenze espresse dagli **Erogatori** nella definizione dei **Requisiti di Fruizione** nel rispetto della protezione dei dati sin dalla progettazione e per impostazione predefinita. Con riferimento all'adesione di persone fisiche, il **Gestore** DEVE informare il richiedente in merito agli attributi **Certificati** che gli verranno associati e alle banche dati ove tali attributi saranno reperiti.

b. **Dichiarati**: sono gli attributi che l'**Aderente**, in veste di **Fruitore**, dichiara di possedere sotto la propria responsabilità al fine di fruire di un determinato **e-service**. Anche tale tipologia di attributi è immediatamente spendibile ai fini della fruizione degli **e-service**, in ragione dell'assunzione di responsabilità del **Fruitore**.

c. **Verificati**: sono gli attributi **Dichiarati** che sono stati verificati da un **Erogatore**. L'**Infrastruttura interoperabilità PDND** assicura la memorizzazione del momento temporale della registrazione di tali attributi.

L'Infrastruttura interoperabilità **PDND** DEVE inserire nel **Registro degli Attributi**:

1. gli **Attributi Certificati** in conformità a quanto indicato alla precedente *lettera a)*;
2. gli attributi proposti dagli **Erogatori** al momento della definizione dei **Requisiti di Fruizione** degli **e-service** pubblicati sul **Catalogo API**.

In relazione all'associazione tra attributi e **Aderenti** e in funzione della fruizione dell'e-service, si precisa che:

- al momento dell'adesione di cui al CAPITOLO 6, l'**Infrastruttura interoperabilità PDND** DEVE associare agli **Aderenti** gli **Attributi Certificati** e assicurarne la persistenza nel tempo in relazione ai dati presenti nelle banche dati di cui alla precedente lettera a);
- l'associazione agli **Aderenti** degli attributi **Dichiarati** e **Verificati** è inserita nel **Registro degli Attributi** a cura, rispettivamente, degli **Aderenti** ed **Erogatori**.

Al momento della definizione dei **Requisiti di Fruizione** dei propri **e-service**, gli **Erogatori DEVONO** verificare se nel **Registro degli Attributi** sono presenti gli **Attributi degli Aderenti** a loro necessari. Effettuata la già menzionata verifica, gli **Erogatori DEVONO**:

- in caso di riscontro positivo, utilizzare gli attributi di proprio interesse, se del caso modificando la tipologia da **Dichiarati** a **Verificati**;
- in caso di riscontro negativo, proporre la definizione di un nuovo attributo, specificando la relativa tipologia richiesta (**Dichiarato** o **Verificato**) e DOVREBBERO associare all'attributo in questione i riferimenti unici presenti nelle banche dati di cui alla precedente lettera a). Ricevuta da un **Erogatore** la proposta di definizione di un nuovo attributo, l'**Infrastruttura interoperabilità PDND** provvede ad aggiungere tale attributo nel **Registro degli Attributi** e a comunicare tale circostanza all'**Erogatore**.

L'Infrastruttura interoperabilità **PDND DEVE** mettere a disposizione del soggetto competente, individuato dalla Presidenza del Consiglio dei ministri, gli strumenti necessari all'ispezione periodica alla ricerca di eventuali attributi equivalenti all'interno **Registro degli Attributi**. Nel caso in cui il soggetto competente constati la presenza di due o più attributi equivalenti, l'**Infrastruttura interoperabilità PDND DEVE** agevolare la comunicazione di tale circostanza agli **Aderenti** interessati e questi ultimi **DEVONO** comunicare le proprie deduzioni sugli attributi equivalenti. In caso di riscontro positivo sull'equivalenza degli attributi a seguito dell'avallo dagli **Aderenti**, l'**Infrastruttura interoperabilità PDND DEVE** agevolare la comunicazione agli **Aderenti** interessati in merito alla normalizzazione dei nomi degli **Attributi degli Aderenti** presenti nel **Registro degli Attributi**.

L'**Infrastruttura interoperabilità PDND** provvede a:

a. aggiornare l'associazione tra gli **Aderenti** e gli **Attributi Certificati** dipendenti dalle variazioni registrate direttamente dalle basi dati di interesse nazionale o altre fonti autoritative utilizzate;
b. recepire le variazioni comunicate dalle fonti autoritative integrate sull'**Infrastruttura interoperabilità PDND** (ad esempio aggiornamento del riferimento normativo, ove segnalato dal sistema **Normattiva**), determinare se gli **Attributi** associati ai riferimenti unici indicati nelle variazioni ricevute sono **Dichiarati** o **Certificati** e segnalare agli **Aderenti** interessati la necessità di valutare l'impatto delle variazioni sopravvenute.

Gli **Aderenti DEVONO** segnalare all'**Infrastruttura interoperabilità PDND** ogni variazione sopravvenuta di cui siano a conoscenza in relazione agli attributi e nello specifico:

- i **Fruitori DEVONO** segnalare le variazioni intervenute sugli attributi **Dichiarati** ad essi associati e sugli attributi **Verificati** da essi indicati;
- gli **Erogatori DEVONO** segnalare le variazioni intervenute sugli attributi **Verificati** con riferimento alla fruizione dei propri **e-service**.

L'**Infrastruttura interoperabilità PDND**, ricevute le segnalazioni di cui sopra, DEVE darne comunicazione agli **Erogatori** interessati, che valutano l'impatto sulla fruizione dei propri **e-service** e comunicano alla **Infrastruttura interoperabilità PDND** le proprie decisioni in merito alla prosecuzione, alla sospensione o al termine dell'erogazione degli **e-service**.

8. Catalogo API

Il **MoDI** individua nelle [LG INTEROPERABILITÀ TECNICA] il **Catalogo API** quale componente, unica e centralizzata, che assicura alle parti coinvolte nel rapporto di erogazione e fruizione la consapevolezza sulle API disponibili e, per ognuna di esse, i livelli di servizio dichiarati.

Il **Catalogo API** permette agli **Erogatori** la registrazione e pubblicazione degli **e-service**, in modo che siano consultabili da tutti gli **Aderenti** e che possa esserne chiesta la fruizione dai **Fruitori** che possiedono gli **Attributi degli Aderenti** coincidenti con i **Requisiti di Fruizione** indicati **dall'Erogatore**.

Il **Catalogo API** è realizzato al fine di:

- favorire l'uso degli **e-service** grazie alla loro pubblicazione e alla messa a disposizione della relativa documentazione tecnica;
- agevolare la gestione del ciclo di vita degli **e-service**;
- mitigare la creazione di interfacce ridondanti e/o con semantica sovrapposta.

La registrazione degli **e-service** è realizzata dagli **Erogatori** che DEVONO:

- assicurare l'utilizzo delle tecnologie e l'applicazione dei pattern e dei profili individuati dal **MoDI** e, in particolare, dalle [LG INTEROPERABILITÀ TECNICA];
- definire i **Requisiti di Fruizione** individuando gli attributi che devono essere posseduti dai **Fruitori** per accedere allo specifico **e-service**, nei casi diversi dagli **e-service** che rendono disponibili dati aperti ai sensi della *Direttiva (UE) 2019/1024*;
- indicare il tempo di durata dei **Voucher** emessi dalla **Infrastruttura interoperabilità PDND** tenuto conto della tipologia dell'**e-service** e dei dati trattati, nel rispetto della normativa in materia di protezione di dati personali;
- indicare che fra i dati oggetto dell'**e-service** rientrano dati personali, come definiti all'art. 4, n. 1) del GDPR.

Nel caso in cui l'**Erogatore** registri un **e-service** che prevede l'applicazione del flusso **Erogazione inversa**, lo stesso **Erogatore DEVE** effettuare, sotto la propria esclusiva responsabilità e tramite gli strumenti messi a disposizione dall'**Infrastruttura interoperabilità PDND**, l'analisi del rischio sulla protezione dei dati personali per ogni specifica finalità per cui dichiara di essere titolato a ricevere i dati da parte di un **Fruitore**. L'analisi del rischio sulla protezione dei dati personali in capo all'**Erogatore** DEVE prevedere gli aspetti indicati al successivo Capitolo 10.

Si precisa che, in merito alle analisi del rischio sulla protezione dei dati personali registrate dai **Fruitori**, l'**Infrastruttura interoperabilità PDND** non è responsabile di quanto ivi dichiarato.

Le informazioni presenti nel **Catalogo API** per ogni **e-service** sono almeno le seguenti:

- descrittori dell'**e-service**, come definiti nell'ALLEGATO 2: PUBBLICAZIONE E FRUIZIONE DELLE API;
- la descrizione dell'API, utilizzando uno degli *interface description language* previsti nelle [LG INTEROPERABILITÀ TECNICA], per usufruire dell'**e-service**;
- la documentazione accessoria e manualistica per l'utilizzo del **e-service**.
- previsione della dichiarazione di una casella di posta, riferita a un'articolazione della struttura organizzativa, che **PUÒ** essere utilizzata dagli **Aderenti** per ricevere e inviare comunicazioni tramite l'**Infrastruttura interoperabilità PDND**.

La registrazione e la correttezza di tali informazioni ricadono nella responsabilità degli **Erogatori**, che **DEVONO** provvedere alla gestione del ciclo di vita dei propri **e-service** (si veda l'ALLEGATO 2: PUBBLICAZIONE

E FRUIZIONE DELLE API) per il tramite dei propri **Utenti degli Aderenti** oppure delegando questo compito a uno o più **Delegati dell'Erogatore**.

Con riferimento al singolo **e-service** registrato nel **Catalogo API**, gli **Erogatori** DEVONO assicurare l'utilizzo di una delle tecnologie indicata dal **MoDI** e, in particolare, dalle [LG INTEROPERABILITÀ TECNICA].

Gli **Erogatori** nell'implementazione dei propri **e-service** al di fuori dell'Infrastruttura interoperabilità PDND **DEVONO**:

a. in caso di **Erogazione Ordinaria**, prevedere nella interfaccia di comunicazione un campo per l'indicazione da parte dei **Fruitori** del riferimento ai documenti informatici (ad esempio numero di protocollo, numero di registrazione, ecc. dell'atto amministrativo che determina la richiesta di accesso ai dati) che possano provare la liceità dello specifico trattamento dei dati personali effettuato in occasione di ogni singolo utilizzo degli **e-service**. In occasione di ogni singolo utilizzo degli **e-service**:
    - il **Fruitore** DEVE comunicare il suddetto riferimento sotto la propria responsabilità;
    - l'**Erogatore** NON DEVE dare seguito alla richiesta del **Fruitore** in assenza del suddetto riferimento.
b. in caso di **Erogazione Inversa**, indicare ai **Fruitori** il riferimento ai documenti informatici (ad esempio numero di protocollo, numero di registrazione, ecc. dell'atto amministrativo che determina la richiesta di accesso ai dati) che possano provare la liceità dello specifico trattamento dei dati personali effettuato in occasione di ogni singolo utilizzo degli **e-service**. In occasione di ogni singolo utilizzo degli **e-service**:
    - l'**Erogatore** DEVE comunicare il suddetto riferimento sotto la propria responsabilità a valle della ricezione dei dati da parte del **Fruitore**.

La raccolta e la memorizzazione di tali riferimenti, considerato che gli scambi dati in ogni circostanza sono realizzati direttamente tra **Erogatore** e **Fruitore**, non avviene sulla **Infrastruttura interoperabilità PDND**.

In caso di **Erogazione Ordinaria**, se il **Fruitore** sia un soggetto privato, il **Fruitore** stesso DEVE permettere agli **Erogatori** di recuperare i documenti che attestino la liceità dello specifico trattamento dei dati personali a partire dal riferimento indicato dal **Fruitore** per la fruizione dell'e-service.

Contestualmente all'utilizzo degli **e-service**:

- il **Fruitore** DEVE memorizzare tutti i documenti che possono provare la liceità del trattamento, associati univocamente al suddetto riferimento, assicurandone l'autenticità e l'integrità;
- l'**Erogatore** DEVE memorizzare la richiesta del **Fruitore** e associarla univocamente al suddetto riferimento, assicurandone l'autenticità e l'integrità.
- il **Fruitore** e l'**Erogatore** DEVONO assicurare, in qualsiasi momento, l'accesso dell'interessato e degli organi di controllo alle informazioni memorizzate.

Gli **Erogatori** DOVREBBERO:

- dare seguito alla metadatazione degli **e-service** utilizzando il modello dati supportato dall'**Infrastruttura interoperabilità PDND**, coerentemente ai vocabolari controllati e alle ontologie definite in attuazione della "strategia nazionale dati" di cui all'articolo 50-ter, comma 4 del CAD;
- utilizzare schemi dati definiti in coerenza con i vocabolari controllati e le ontologie definiti in attuazione della "strategia nazionale dati" di cui all'articolo 50-ter, comma 4 del **CAD** per la metadatazione dei dati oggetto dei propri **e-service** nelle modalità supportate dall'**Infrastruttura interoperabilità PDND**.

Relativamente agli **e-service** pubblicati, gli **Erogatori** NON POSSONO modificare elementi che impattano sui **Fruitori** e NON POSSONO dismettere una versione di **e-service** in costanza di fruizione.

L'*Allegato 2: Pubblicazione e fruizione delle API* individua nello specifico le modalità che gli **Erogatori** DEVONO attuare per registrare, pubblicare e aggiornare le informazioni relative ai propri **e-service** sul **Catalogo API** nonché le modalità che i **Fruitori** DEVONO attuare per consultare l'elenco degli **e-service** pubblicati sul **Catalogo API**.

9. Richiesta di fruizione di e-service

Un **Aderente** che intende fruire di un **e-service** pubblicato da un **Erogatore DEVE**, nei casi diversi dagli **e-service** che rendono disponibili dati aperti ai sensi Direttiva (UE) 2019/1024, dare seguito ad una richiesta di fruizione attraverso i seguenti passaggi:

1. l'**Aderente** individua l'**e-service** di proprio interesse fra quelli presenti nel **Catalogo API**;
2. l'**Aderente** invia all'**Erogatore** per il tramite dell'**Infrastruttura interoperabilità PDND** la richiesta di fruizione dell'**e-service**, nella quale **DEVE** dichiarare - ove non effettuato precedentemente - il possesso degli eventuali attributi **Dichiarati** e/o di quelli **Verificati** necessari a soddisfare i **Requisiti di Fruizione** stabiliti dall'**Erogatore** per lo specifico **e-service**;
3. qualora per la fruizione dell'**e-service** siano previsti **Attributi Verificati** dichiarati dall'**Aderente**, l'**Erogatore DEVE** verificarne il possesso da parte dell'**Aderente**.

L'**Infrastruttura interoperabilità PDND DEVE** rendere disponibili agli **Aderenti**, o ai **Delegati dei Fruitori** degli stessi, le funzionalità per attuare i passaggi indicati in precedenza.

La richiesta di fruizione di un **e-service** è conclusa con esito positivo se risultano soddisfatte le seguenti condizioni:

a. all'**Aderente** sono associati **Attributi** certificati tali da soddisfare i **Requisiti di Fruizione** stabiliti dall'**Erogatore** per lo specifico **e-service**;
b. l'**Aderente** ha dichiarato **Attributi** dichiarati, così come indicato al precedente passaggio 2, tali da soddisfare, eventualmente in combinazione con gli **Attributi** certificati associati allo stesso **Aderente**, i **Requisiti di Fruizione** stabiliti dall'**Erogatore** per lo specifico **e-service**;
c. l'**Aderente** ha dichiarato **Attributi** verificati, così come indicato al precedente passaggio 1, e gli stessi sono stati verificati dall'**Erogatore** dell'**e-service**, così come indicato al precedente passaggio 3, tali da soddisfare, eventualmente in combinazione con gli **Attributi** certificati associati allo stesso **Aderente** e/o con gli **Attributi** dichiarati dallo stesso **Aderente**, i **Requisiti di Fruizione** stabiliti dall'**Erogatore** per lo specifico **e-service**.

A fronte di una richiesta di fruizione per un e-service che richieda un'azione esplicita per essere accettata da parte dell'**Erogatore**, il **Gestore** comunica la creazione della richiesta allo stesso **Erogatore**. Ai sensi della Legge 241/1990, ove siano trascorsi 30 giorni da quando il **Fruitore** ha inviato una richiesta di fruizione all'**Erogatore**, senza che quest'ultimo vi abbia dato seguito, il **Gestore** DEVE inviare una comunicazione all'**Erogatore** per segnalare la richiesta di fruizione rimasta inevasa.

L'**Infrastruttura interoperabilità PDND** DEVE assicurare agli **Aderenti** l'accesso ai dati relativi alle richieste di fruizione di cui sono parte, come **Erogatori** o **Fruitori**, e in particolare:

- permetterne la sospensione o eliminazione nei casi in cui risultino decaduti i presupposti che ne hanno determinato l'esito positivo e/o nell'ipotesi in cui gli **Aderenti** riscontrino usi impropri degli **e-service**;
- recuperarli nella forma di documento informatico, assicurando l'integrità dei dati e la certezza della loro origine.

L'**Infrastruttura interoperabilità PDND** NON DEVE emettere **Voucher** per richieste di fruizione sospese o eliminate dagli **Aderenti**.

10. Analisi del rischio sulla protezione dei dati personali e configurazione del servizio di erogazione

A valle della positiva conclusione della richiesta di fruizione di un **e-service** da parte di un **Fruitore**, così come indicato al precedente Capitolo 9 Richiesta di fruizione di e-service, ove gli **e-service** veicolino dati personali e nei casi diversi dagli **e-service** che rendono disponibili dati aperti ai sensi Direttiva (UE) 2019/1024:

a. in caso di **Erogazione Ordinaria**, il **Fruitore** DEVE effettuare, sotto la propria esclusiva responsabilità e tramite gli strumenti messi a disposizione dall'**Infrastruttura interoperabilità PDND**, l'analisi del rischio sulla protezione dei dati personali con riferimento ad ogni specifica Finalità per cui intende presentare una richiesta di fruizione dell'**e-service**;
b. in caso di **Erogazione Inversa**, il **Fruitore** DEVE selezionare l'analisi del rischio correlata alla specifica finalità per cui intende trasmettere i dati, fra quelle disponibili;

Qualora la fruizione di un **e-service** comporti un trattamento di dati personali, l'**Erogatore** è tenuto a configurare gli **e-service** adottando misure tecniche e organizzative nel rispetto dei principi di liceità, correttezza e sicurezza del trattamento, adeguate alle caratteristiche degli stessi (ad esempio, se del caso, il tracciamento delle operazioni svolte dai singoli operatori del Fruitore e l'attivazione di meccanismi di alerting).
In particolare, l'**Erogatore** è tenuto a vigilare sugli accessi alle proprie banche dati, anche con attività di monitoraggio costante delle chiamate ricevute dal **Fruitore** e controlli a campione sulla validità delle analisi del rischio compilate, a cui il **Fruitore** è tenuto a collaborare. Il **Fruitore** è tenuto a rispettare i **Requisiti di Fruizione**, tra cui quelli riferibili alle misure tecniche e organizzative individuate dall'**Erogatore** (ad esempio, l'esecuzione di specifici controlli e il riscontro tempestivo a eventuali segnalazioni di anomalia pervenute dall'Erogatore). Una volta acquisiti i dati per il tramite dell'**Infrastruttura interoperabilità PDND**, il **Fruitore,** in qualità di titolare del trattamento, è responsabile dell'adozione di misure tecniche e organizzative adeguate affinché il trattamento di tali dati avvenga nel rispetto dei principi di liceità, correttezza e sicurezza e in conformità alle finalità dichiarate.

Nel caso di **Erogazione Ordinaria** in cui l'**e-service** erogato non prevede il trattamento di dati personali, come indicato dell'**Erogatore** al momento della pubblicazione dello stesso **e-service**, l'analisi del rischio a carico del **Fruitore** PUÒ essere semplificata.

Nel caso di **Erogazione Inversa** in cui l'**Erogatore** attesti che l'**e-service** dallo stesso pubblicato non effettui trattamento dei dati personali, l'analisi del rischio a suo carico **PUÒ** essere semplificata.

Il **Fruitore** in ogni caso deve dichiarare sull'**Infrastruttura interoperabilità PDND** una casella di posta, riferita a un'articolazione della struttura organizzativa, per permettere all'**Erogatore** di contattarlo direttamente.

Per agevolare la compilazione dell'analisi del rischio, il **Gestore** PUÒ rendere disponibili sull'Infrastruttura interoperabilità **PDND** modelli precompilati per determinate finalità, pur rimanendo estraneo alla loro redazione. Il **Gestore** DEVE consentire in ogni caso la modifica dei campi precompilati e non è responsabile per le informazioni e dati contenuti nei modelli precompilati.

L'analisi del rischio sulla protezione dei dati personali DEVE prevedere almeno i seguenti aspetti:

- individuazione della base giuridica del trattamento dei dati personali oggetto della fruizione dell'**e-service**, ai sensi dell'articolo 6 del GDPR;
- dichiarazione della finalità per cui il **Fruitore** intende accedere ai dati personali messi a disposizione mediante l'**e-service**; qualora sussista più di una finalità, il **Fruitore** DEVE effettuare un'analisi del rischio per ognuna delle finalità individuate;
- analisi in merito all'effettivo rispetto dei principi di cui all'art. 5 del GDPR e di quanto disposto all'art. 25 del GDPR nella fruizione dell'**e-service** per la specifica finalità dichiarata;
- conferma dell'avvenuta individuazione del periodo di conservazione dei dati personali ottenuti mediante la fruizione dell'**e-service**.

Il **Fruitore** DEVE altresì indicare la stima di carico in relazione alle richieste che effettuerà all'**e-service** in merito alla specifica finalità.

In tale contesto **Erogatore** e **Fruitore**, al di fuori dell'Infrastruttura interoperabilità **PDND**, POSSONO concordare specifici SLA per l'erogazione dell'**e-service** e registrarli sulla **Infrastruttura interoperabilità PDND**.

A seguito dell'indicazione della stima di carico, l'**Infrastruttura interoperabilità PDND**, nell'ipotesi in cui la richiesta del **Fruitore** ecceda la stima di carico precedentemente dichiarata dall'**Erogatore**, DEVE comunicare all'**Erogatore** quanto registrato dal **Fruitore** e provvedere a registrare la specifica finalità indicata dal **Fruitore** per la fruizione dello specifico **e-service** solo a seguito della conferma dell'**Erogatore** in relazione all'eventuale completamento delle configurazioni dei propri sistemi informatici necessarie ad assolvere alle richieste del **Fruitore**. Nel caso in cui l'**Erogatore** reputi non possibile dare seguito alla richiesta di un **Fruitore** eccedente le stime di carico precedentemente indicate da esso DEVE comunicare al **Fruitore**, per il tramite l'**Infrastruttura interoperabilità PDND**, le circostanze che non rendono soddisfacibile la stessa richiesta inoltrata da questo.

Si precisa che, in merito alle analisi del rischio sulla protezione dei dati personali registrate dai **Fruitori**, l'**Infrastruttura interoperabilità PDND** non è responsabile di quanto ivi dichiarato.

Il **Fruitore**, al variare delle proprie esigenze, **PUÒ**:

a. sospendere o eliminare una finalità precedentemente registrata sulla **Infrastruttura interoperabilità PDND**;
b. ridurre l'indicazione della stima di carico di una specifica finalità precedentemente registrata sulla **Infrastruttura interoperabilità PDND**;
c. aumentare l'indicazione della stima di carico di una specifica finalità precedentemente registrata sulla **Infrastruttura interoperabilità PDND**, ferma restando la conferma dell'**Erogatore** in relazione all'eventuale completamento delle configurazioni dei propri sistemi informatici necessario ad assolvere alle richieste del **Fruitore**, fatti salvi i casi in cui la nuova richiesta non ecceda la disponibilità precedentemente dichiarata dall'Erogatore.

L'**Infrastruttura interoperabilità PDND DEVE** assicurare agli **Aderenti** l'accesso ai dati relativi alle analisi del rischio sulla protezione dei dati personali e alle configurazioni dei servizi di erogazione per singola finalità di fruizione in cui sono parte, come **Erogatori** o **Fruitori**, e in particolare:

- permettere la sospensione o il blocco dell'utilizzo dell'**e-service** per la singola finalità di fruizione nell'ipotesi in cui gli **Aderenti** riscontrino usi impropri degli **e-service**;
- recuperare i dati nella forma di documento informatico, assicurando l'integrità dei dati e la certezza della loro origine.

L'**Infrastruttura interoperabilità PDND DEVE** rendere disponibili agli **Aderenti**, o agli **Delegati dei Fruitori** degli stessi, le funzionalità per attuare i passaggi indicati in precedenza.

L'**Infrastruttura interoperabilità PDND NON DEVE** emettere **Voucher** per singola finalità di fruizione sospesa o bloccata dagli **Aderenti**.

11. Responsabilità

Il **Gestore**, l'**Erogatore** e il **Fruitore** DEVONO operare nel rispetto delle disposizioni di cui alle presenti **Linee guida** e ai relativi Allegati.

Tutte le dichiarazioni rese dagli **Aderenti** nelle interazioni con e tramite l'**Infrastruttura interoperabilità PDND** si intendono rese ai sensi del D.P.R. 445/2000.

Con riferimento alla fruizione della **Infrastruttura interoperabilità PDND**, in particolare, il **Gestore** DEVE:

a. garantire i livelli di servizio concordati con l'**Aderente** nell'**Accordo di adesione**;
b. conservare tutte le evidenze digitali necessarie ad attestare in maniera certa le attività svolte dagli **Aderenti**;
c. adottare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, sorvegliare e tracciare l'accesso e le attività dei propri utenti per il tempo strettamente necessario e anche al fine di tutelare la protezione dei dati personali secondo quanto definito dagli artt. 25, 29 e 32 del GDPR, informando, senza ingiustificato ritardo, gli **Aderenti** interessati in caso di violazioni di sicurezza o di qualsiasi minaccia che comporti un rischio per la sicurezza e per i diritti e le libertà degli interessati.

L'**Erogatore** DEVE garantire, essendo nella sua esclusiva responsabilità:

a. la conformità dell'**e-service** alla normativa vigente, anche in tema di protezione dei dati personali, tenuto conto in particolare della protezione dei dati sin dalla progettazione e per impostazione predefinita di cui all'art. 25 del GDPR, nonché effettuando un'analisi del rischio per i diritti e le libertà delle persone fisiche e, qualora sussistano le condizioni di cui agli artt. 35 e 36 del GDPR, altresì la valutazione d'impatto sulla protezione dei dati personali e l'eventuale consultazione preventiva;
b. l'accesso all'**e-service** e la relativa fruizione da parte del **Fruitore** che possieda gli **Attributi** richiesti e, in caso di **Erogazione Ordinaria**, che abbia compilato l'analisi del rischio sulla protezione dei dati personali;
c. in caso di **Erogazione Inversa**:
    i. la compilazione dell'analisi del rischio sulla protezione dei dati personali che saranno ottenuti mediante l'erogazione dell'**e-service**, compilando tutti i campi dello strumento messo a disposizione dall'Infrastruttura interoperabilità **PDND** con riferimento a ogni specifica finalità di fruizione dell'**e-service**;
    ii. l'utilizzo dei dati e delle informazioni di cui entrerà in possesso in fase di erogazione dell'**e-service** solo per le finalità dichiarate e nei limiti di queste nonché unicamente per il tempo strettamente necessario allo svolgimento delle attività per cui ne è stata richiesta la fruizione;
d. la minimizzazione, l'esattezza, l'integrità e la riservatezza dei dati comunicati al **Fruitore** in fase di erogazione dell'**e-service**;
e. il tracciamento degli accessi e delle operazioni effettuate, come individuati nelle presenti **Linee Guida** e associati alla fruizione dell'**e-service**, nonché la relativa conservazione per il tempo strettamente necessario;
f. l'adozione di misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, sorvegliare e tracciare l'accesso e le attività dei propri utenti per il tempo strettamente necessario e al solo fine di tutelare la protezione dei dati personali secondo quanto definito dagli artt. 25, 29 e 32 del GDPR, informando tempestivamente i **Fruitori** interessati, anche per il tramite dell'**Infrastruttura Interoperabilità PDND**, in caso di violazioni di sicurezza o di qualsiasi minaccia che comporti un rischio per la sicurezza e per i diritti e le libertà degli interessati;

g. la conservazione, a fini probatori, dei **Voucher** emessi dall'**Infrastruttura Interoperabilità PDND** per l'accesso ai propri **e-service**.

Il **Fruitore** DEVE, essendo nella sua esclusiva responsabilità:

a. richiedere la fruizione dell'e-service di proprio interesse, solo laddove ritenga di possedere tutti gli **Attributi Certificati**, **Dichiarati** e **Verificati** previsti nei **Requisiti di fruizione** dell'**e-service**;
b. in caso di **Erogazione Ordinaria**, effettuare l'analisi del rischio sulla protezione dei dati personali dei trattamenti che si intende intraprendere con la fruizione dell'**e-service**, compilando tutti i campi dello strumento messo a disposizione dall'**Infrastruttura interoperabilità PDND** con riferimento a ogni specifica finalità di fruizione dell'**e-service**;
c. in caso di **Erogazione Inversa**, dopo la compilazione dell'analisi del rischio da parte dell'**Erogatore**, selezionare l'analisi del rischio correlata alla specifica finalità per cui intende comunicare i dati, fra quelle disponibili;
d. in caso di **Erogazione Inversa**, effettuare un'analisi del rischio per i diritti e le libertà delle persone fisiche e, qualora sussistano le condizioni di cui agli artt. 35 e 36 del GDPR, altresì la valutazione d'impatto sulla protezione dei dati personali e l'eventuale consultazione preventiva;
e. in caso di **Erogazione Ordinaria**, comunicare direttamente all'**Erogatore** il riferimento ai documenti informatici (ad esempio numero di protocollo, numero di registrazione, ecc. dell'atto amministrativo che determina la richiesta di accesso ai dati) che dimostrino la sussistenza del rapporto intercorrente con il soggetto di cui sono richiesti i dati personali e che consenta di accedere legittimamente a tutti i dati e le informazioni messi a disposizione dall'**Erogatore** tramite l'**e-service**;
f. in caso di **Erogazione Inversa**, ricevere direttamente dall'**Erogatore** il riferimento ai documenti informatici (ad esempio numero di protocollo, numero di registrazione, ecc. dell'atto amministrativo che determina la richiesta di accesso ai dati) che dimostrino la sussistenza del rapporto intercorrente con il soggetto di cui l'**Erogatore** riceverà dati personali e che gli consente di accedervi legittimamente;
g. in caso di **Erogazione Inversa**, garantire la minimizzazione, l'esattezza, l'integrità e la riservatezza dei dati comunicati all'**Erogatore** in fase di fruizione dell'**e-service**;
h. utilizzare i dati e le informazioni di cui entrerà in possesso in fase di fruizione dell'**e-service** solo per la/e finalità dichiarata/e nei limiti di questa/e nonché unicamente per il tempo strettamente necessario allo svolgimento delle attività per cui ne è stata richiesta la fruizione;
i. su richiesta dell'**Erogatore**, aderire alle eventuali successive versioni dell'e-service predisposte e rilasciate sul **Catalogo API**, entro il periodo di tempo indicato dall'**Erogatore** con specifica comunicazione, e provvedere conseguentemente a dismettere la versione precedente dell'e-service;
j. individuare, all'interno della propria organizzazione e accreditare sull'**Infrastruttura interoperabilità PDND**, gli **Utenti** autorizzati a operare per proprio conto con riferimento alla gestione del singolo **e-service**, provvedendo a formarli ai sensi della normativa vigente in tema di protezione dei dati personali;
k. comunicare tempestivamente all'**Erogatore** eventuali sopravvenute criticità che impattino sulla fruizione dell'**e-service**;
l. comunicare immediatamente all'**Erogatore** il verificarsi di eventi che impattino sulla sicurezza della fruizione dell'**e-service**;
m. segnalare immediatamente all'**Erogatore** qualsiasi malfunzionamento o disservizio riscontrato in fase di accesso e/o fruizione dell'**e-service**;
n. in caso di violazione dei dati personali, procedere all'eventuale notifica all'Autorità di controllo e, ove necessario, alla comunicazione agli interessati in applicazione degli artt. 33 e 34 del GDPR;
o. adottare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, sorvegliare e tracciare l'accesso e le attività dei propri utenti per il tempo strettamente necessario e

al solo fine di tutelare la protezione dei dati personali secondo quanto definito dagli artt. 25, 29 e 32 del GDPR, informando tempestivamente gli **Erogatori** interessati, anche per il tramite dell'**Infrastruttura Interoperabilità PDND**, in caso di violazioni di sicurezza o di qualsiasi minaccia che comporti un rischio per la sicurezza e per i diritti e le libertà degli interessati;

p. dotarsi degli strumenti e di tutte le soluzioni informatiche necessarie a un uso ottimale delle funzionalità di fruizione dell'**e-service**;
q. controllare e garantire la sicurezza degli accessi all'**e-service**, tenuto conto che il tracciamento applicativo degli accessi e delle operazioni effettuate è svolto anche dall'**Erogatore**;
r. conservare, a fini probatori, i **Voucher** ricevuti dall'Infrastruttura Interoperabilità per accedere agli **e-service** degli **Erogatori**.

In caso di mancato rispetto degli obblighi sopra previsti in capo al **Fruitore**, l'**Erogatore** PUÒ sospendere la fruizione dell'**e-service** anche con effetto immediato, disattivando temporaneamente o permanentemente la possibilità del **Fruitore** di accedere all'e-service.

12. Trust Infrastruttura interoperabilità PDND e sistemi informatici degli Aderenti

Per il tramite delle funzionalità rese disponibili dall'**Infrastruttura interoperabilità PDND** è realizzato il trust machine-to-machine tra:

- sistemi informatici degli **Aderenti** e sistemi informatici della **Infrastruttura interoperabilità PDND**;
- sistemi informatici degli **Aderenti**.

Gli **Aderenti DEVONO** generare il materiale crittografico utilizzato nel trust e assicurarne la riservatezza, adottando adeguate misure di sicurezza tecniche e organizzative che preservino tale materiale da un utilizzo improprio.

Gli **Aderenti DEVONO** registrare e mantenere sull'**Infrastruttura interoperabilità PDND** il materiale crittografico pubblico utilizzato dai propri sistemi informatici che interagiranno con la **Infrastruttura interoperabilità PDND** e i sistemi informatici degli altri **Aderenti**.

L'**Infrastruttura interoperabilità PDND DEVE** generare il proprio materiale crittografico utilizzato dagli **Aderenti** per verificare l'autenticità dei **Voucher** e assicurare la riservatezza di tale materiale crittografico, adottando adeguate misure di sicurezza tecniche e organizzative che preservino tale materiale da un utilizzo improprio.

L'**Infrastruttura interoperabilità PDND DEVE** rendere disponibile agli **Aderenti** il materiale crittografico pubblico necessario alla verifica dei **Voucher** emessi dalla stessa.

L'**Infrastruttura interoperabilità PDND** deve altresì distribuire il materiale crittografico pubblico depositato sulla infrastruttura stessa dagli **Aderenti** e, all'interno delle comunicazioni machine-to-machine, garantire l'utilizzo dello stesso per consentire:

- la creazione di canali sicuri machine-to-machine tra **Fruitore** ed **Erogatore**;
- la verifica da parte dell'**Erogatore** dell'integrità delle richieste inviate dal **Fruitore**;
- la verifica da parte del **Fruitore** dell'integrità delle risposte inviate dall'**Erogatore**;

Per dare seguito alle transazioni tra **Erogatore** e **Fruitore** con riferimento a un determinato **e-service**, i sistemi informatici degli stessi **DEVONO** realizzare i seguenti passi:

1. il sistema informatico del **Fruitore** richiede all'**Infrastruttura interoperabilità PDND** l'emissione di un **Voucher** riconducibile alla richiesta di fruizione dell'**e-service** e alla relativa analisi del rischio, utilizzando il materiale crittografico registrato sull'**Infrastruttura interoperabilità PDND**;
2. l'**Infrastruttura interoperabilità PDND** emette un **Voucher**, con validità temporale limitata, contenente le informazioni necessarie a identificare il **Fruitore** e la specifica richiesta di fruizione con correlata analisi del rischio, utilizzando il materiale crittografico a tal fine generato dalla stessa **Infrastruttura**;
3. il sistema informatico del **Fruitore** utilizza il **Voucher** per chiedere al sistema informatico dell'**Erogatore** la fruizione dell'**e-service**;
4. il sistema informatico dell'**Erogatore**, ricevuto il **Voucher**, utilizzando il materiale crittografico pubblico registrato sull'**Infrastruttura interoperabilità PDND**, ne verifica l'emissione da parte dell'**Infrastruttura interoperabilità PDND** e la relativa validità temporale e, solo in caso di esito positivo della verifica, abilita il sistema informatico del **Fruitore** alla fruizione dell'**e-service**.

L'**Erogatore** al momento della definizione dell'**e-service PUÒ** prevedere tra i **Requisiti di Fruizione** che il sistema informatico del **Fruitore** sia identificato direttamente al precedente passo 4. In questo caso il **Fruitore** utilizza, al precedente passo 3, il materiale crittografico registrato sull'**Infrastruttura interoperabilità PDND** per decorare il **Voucher** per permettere all'**Erogatore** di identificarlo.

Le tecnologie utilizzate per l'implementazione dei **Voucher** che l'**Infrastruttura interoperabilità PDND DEVE** assicurare sono indicate nell'ALLEGATO 3: STANDARD E DETTAGLI TECNICI UTILIZZATI PER LA FRUIZIONE DEI VOUCHER DI AUTORIZZAZIONE.

Gli **Aderenti DEVONO** implementare i passi indicati in precedenza per il tramite dell'**Infrastruttura interoperabilità PDND** nelle modalità indicate nell'ALLEGATO 3: STANDARD E DETTAGLI TECNICI UTILIZZATI PER LA FRUIZIONE DEI VOUCHER DI AUTORIZZAZIONE.

13. Raccolta delle informazioni relative agli accessi e alle transazioni

L'**Infrastruttura interoperabilità PDND DEVE** fornire supporto per il tracciamento e l'osservazione delle interazioni tra **Erogatori** e **Fruitori** e colleziona alcune informazioni utili a misurare l'efficacia dell'interoperabilità nel tempo, senza supporto alla valutazione degli SLA eventualmente concordati tra **Erogatori** e **Fruitori**.

In particolare, l'articolo 50-ter, comma 2, del **CAD** stabilisce che l'**Infrastruttura interoperabilità PDND** rende possibile l'interoperabilità dei sistemi informativi e delle basi di dati anche mediante *"la raccolta e conservazione delle informazioni relative agli accessi e alle transazioni effettuate suo tramite"*.

A tal fine, i servizi previsti includono:

- **Probing:** verifica periodica della disponibilità delle API presenti nel relativo Catalogo e dichiarate "in erogazione". L'**Erogatore DEVE** includere nella firma dell'e-service una chiamata di monitoraggio, secondo le indicazioni presenti nella documentazione tecnica caricata sul portale della **Infrastruttura interoperabilità PDND** a cura del **Gestore**. L'**Infrastruttura Interoperabilità PDND** conserva, anche in maniera aggregata, gli esiti delle chiamate almeno in termini di:
  - successo/fallimento;
  - coordinate temporali.
- **Auditing:** registrazione delle autorizzazioni (Voucher) rilasciate dalla **Infrastruttura Interoperabilità PDND** su richiesta dei **Fruitori**. L'**Infrastruttura interoperabilità PDND DEVE** conservare per ogni evento di autorizzazione almeno:
  - le coordinate temporali del rilascio del **Voucher**;
  - il riferimento alla richiesta di fruizione dell'**e-service** e alla relativa analisi del rischio;
  - la finalità entro cui saranno realizzate le transazioni;
  - l'URL dell'API richiesta;
  - eventuali parametri con cui il **Fruitore** decora la richiesta di autorizzazione per l'emissione del Voucher.
- **Tracing**: un servizio di raccolta dei tracciati che descrivono l'andamento esclusivamente quantitativo delle transazioni avvenute tra ciascun **Erogatore** e ciascun **Fruitore**. L'**Erogatore DEVE** assicurare l'inoltro delle informazioni a tale servizio, senza comprendere il contenuto informativo scambiato, così da consentire di descrivere il numero di transazioni intervenute tra **Erogatore** e **Fruitore** in un determinato arco di tempo. Gli **Erogatori DEVONO** depositare i tracciati con le modalità e le tempistiche indicate nella documentazione tecnica prodotta dal **Gestore**.
  Le informazioni depositate dagli **Erogatori** sull'**Infrastruttura interoperabilità PDND DEVONO** essere aggregate almeno in base ai seguenti criteri:
  - coordinate temporali con la granularità che sarà definita dal **Gestore della Piattaforma**;
  - **Aderenti** coinvolti nella transazione e loro ruolo;
  - **e-service** oggetto della richiesta di fruizione;
  - esito della chiamata/risposta.

  Ulteriori criteri di aggregazione delle informazioni depositate dagli **Erogatori** sull'**Infrastruttura interoperabilità PDND** potranno essere definiti dal **Gestore**.

L'obiettivo della **Infrastruttura interoperabilità PDND** resta ancorato alla realizzazione di un punto unico di raccolta di queste informazioni, non essendo tenuta a svolgere un compito di riconciliazione dei tracciati di una stessa transazione e provenienti da **Aderenti** diversi.

14. Garanzia dell'interoperabilità semantica dei contenuti

Per assicurare la qualità dei dati presenti nell'**Infrastruttura interoperabilità PDND** nell'ALLEGATO 7: REGOLE DI POPOLAMENTO sono definite le regole di popolamento degli attributi delle entità (descrittore degli e-service, richiesta di fruizione e-service, finalità per l'accesso agli e-service, …) registrate sulla stessa.

Una singola regola di popolamento presente nell'ALLEGATO 7: REGOLE DI POPOLAMENTO:

1. **DEVE** afferire ad uno specifico attributo di una singola entità registrata nell'**Infrastruttura interoperabilità PDND;**
2. **DEVE** essere definita, sentito il **Gestore**, e verificabile attraverso controlli automatici applicabili ex-ante sulle entità già registrate nell'**Infrastruttura interoperabilità PDND;**
3. **DEVE** essere coerente con i vocabolari controllati e modelli di dati definiti a livello nazionale e internazionale.

Gli **Aderenti DEVONO** assicurare la corretta applicazione delle regole di popolamento presenti nell'ALLEGATO 7: REGOLE DI POPOLAMENTO al momento del popolamento delle entità sull'**Infrastruttura interoperabilità PDND**.

L'**Infrastruttura interoperabilità PDND DEVE** implementare le regole di popolamento presenti nell'ALLEGATO 7: REGOLE DI POPOLAMENTO impedendo agli **Aderenti** il popolamento delle entità per cui almeno una delle regole di popolamento è violata.

L'**Infrastruttura interoperabilità PDND DEVE** implementare gli strumenti per permettere agli **Aderenti** di correggere le entità già registrate per cui si evidenzia la violazione di una o più regole di popolamento presenti nell'ALLEGATO 7: REGOLE DI POPOLAMENTO.

Il **Gestore DEVE** rendere disponibile alla Presidenza del Consiglio dei Ministri, o al soggetto dalla stessa delegata, le evidenze dei popolamenti delle entità effettuate dagli **Aderenti** sull'**Infrastruttura interoperabilità PDND** per cui le regole di popolamento non sono soddisfatte.

L'ALLEGATO 7: REGOLE DI POPOLAMENTO è aggiornato nei modi previsti al capitolo 5 – Processo di aggiornamento degli Allegati fatto salvo che l'esigenza che determina l'aggiornamento dello stesso allegato **DEVE** essere segnalata ad AgID dalla Presidenza del Consiglio dei ministri, o dal soggetto dalla stessa delegata.

A seguito di un aggiornamento dell'ALLEGATO 7: REGOLE DI POPOLAMENTO il **Gestore DEVE** rendere disponibile alla Presidenza del Consiglio dei Ministri, o al soggetto dalla stessa delegata, le entità popolate dagli **Aderenti** sull'**Infrastruttura interoperabilità PDND** per cui le regole di popolamento non sono soddisfatte.

15. Livelli di servizio dell'Infrastruttura interoperabilità PDND

Il rapporto tra il **Gestore** e gli **Aderenti** è regolato dai livelli di qualità, oggetto dell'ALLEGATO 1: PROCESSO DI ADESIONE E ACCORDO DI ADESIONE, attesi nell'erogazione dei:

- servizi offerti agli **Aderenti** per la gestione degli **e-service** e **Voucher** assicurati dalla **Infrastruttura interoperabilità PDND**;
- servizi di supporto agli **Utenti degli Aderenti** da parte della **Infrastruttura interoperabilità PDND**.

In quanto segue si riportano gli indicatori di qualità utilizzati dalla **Infrastruttura interoperabilità PDND** e dagli **Aderenti** per definire i livelli di qualità dei servizi che l'**Infrastruttura interoperabilità PDND** garantisce agli **Aderenti**, oggetto dell'Allegato sull'**Accordo di Adesione**.

15.1. Indicatori dei servizi/API realizzati

15.1.1. Tempo di risposta delle richieste su percentile

Il tempo che intercorre tra una request e la relativa response, è indice dell'efficienza di un servizio/API reso disponibile dall'**Infrastruttura interoperabilità PDND**. Nel dettaglio il tempo di risposta è calcolato, in esercizio, come il tempo intercorso tra il momento di ricezione della request e il momento di inoltro della relativa response. Le latenze determinate dal canale di comunicazione del servizio/API non sono oggetto del presente indicatore.

Il presente indicatore è determinato dalla media di un percentile fissato delle request pervenute nell'unità di tempo, dove il percentile e l'unità di tempo per la determinazione dell'indicatore sono individuate nell'**Accordo di Adesione** sottoscritta dall'**Infrastruttura interoperabilità PDND** e dagli **Aderenti** per singolo servizio/API, ad esempio tempo medio dell'85% delle richieste pervenute in 10 minuti.

La fonte per la determinazione dei tempi di ricezione delle request e il momento di inoltro delle relative response è rappresentato dai log file tenuti dall'**Infrastruttura interoperabilità PDND**.

15.1.2. Numero di richieste per unità di tempo

Il numero di richieste soddisfatte da un servizio/API reso disponibile dall'Infrastruttura interoperabilità **PDND** è indice della capacità di carico gestibile dalla stessa.

Il presente indicatore è determinato dal numero di request soddisfate, cioè a cui il servizio/API è riuscito a produrre response, nell'unità di tempo. L'unità di tempo per la determinazione dell'indicatore è individuata nell'**Accordo di Adesione** sottoscritta dall'Infrastruttura interoperabilità **PDND** e dagli **Aderenti** per singolo servizio/API, ad esempio numero di request soddisfatte in 10 minuti.

La fonte per la determinazione del numero di request soddisfatte è rappresentata dai log file tenuti dall'**Infrastruttura interoperabilità PDND**.

15.1.3. Numero di richieste con risposta di errore per unità di tempo

Il numero di richieste con risposta di errore di un servizio/API reso disponibile dall'**Infrastruttura interoperabilità PDND** è indice inverso dell'efficacia della stessa.

Il presente indicato è determinato del numero di request con error response nell'unità di tempo, escludendo gli errori imputabili agli **Aderenti** (ad esempio errata formattazione della richiesta o la irraggiungibilità dei servizi degli **Aderenti**). L'unità di tempo per la determinazione dell'indicatore è individuata nell'**Accordo di Adesione** sottoscritta dall'**Infrastruttura interoperabilità PDND** e dagli **Aderenti** per singolo servizio/API,

ad esempio numero di request con error response in 10 minuti. Si evidenzia che tale indicatore è inversamente proporzionale all'efficacia del servizio/API.

La fonte per la determinazione del numero di request con error response è rappresentata dai log file tenuti dalla **Infrastruttura interoperabilità PDND**.

15.2. Indicatori dei servizi di supporto

15.2.1. Tempestività di ripristino dell'operatività

Il presente indicatore si applica a non conformità funzionali e non funzionali rilevate dagli **Aderenti** ed è calcolato come la differenza in ore tra il momento dell'avvio del processo di risoluzione del malfunzionamento e il termine della risoluzione delle stesso da parte della **Infrastruttura interoperabilità PDND**.

La fonte per la determinazione dell'indicatore è rappresentata dal momento temporale della presa in carico della segnalazione da parte del **Gestore**.

15.2.2. Tempestività di risposta a segnalazioni di anomalie

Il presente indicatore si applica a non conformità funzionali e non funzionali evidenziate dagli **Aderenti**. L'indicatore è calcolato come la differenza in ore tra il momento della segnalazione e la presa in carico della stessa da parte dell'**Infrastruttura interoperabilità PDND**.

La fonte per la determinazione dell'indicatore è rappresentata dal momento temporale della presa in carico della segnalazione da parte del **Gestore**.

16. Distribuzione dei segnali di variazione degli stati e dei fatti

L'**Infrastruttura interoperabilità PDND** ha il ruolo di raccogliere e distribuire gli eventi che un **Aderente**, nel ruolo di **Produttore**, genera con lo scopo di comunicare ad altri **Aderenti**, nel ruolo di **Consumatore**, la presenza di variazioni degli stati e fatti conosciuti all'interno del suo dominio relativamente ad uno specifico **e-service** pubblicato dall'**Aderente produttore** e fruito dall'**Aderente consumatore**.

Gli standard e le tecnologie, comprese le funzioni di hashing per la pseudonimizzazione, utilizzati per dare seguito alla generazione degli eventi di variazione da parte degli **Aderenti produttori** e la divulgazione agli **Aderenti consumatori** sono oggetto dell'ALLEGATO 4: PROCESSO DI DISTRIBUZIONE DEI SEGNALI DI VARIAZIONE.

L'**Infrastruttura interoperabilità PDND** distribuisce gli eventi generati, i **Segnali di Variazione**, da un **Aderente produttore** per un suo **e-service** attivo solo ed esclusivamente agli **Aderenti consumatori** che hanno almeno una finalità attiva per tale **e-service**.

I **Segnali di Variazione** non trasportano né il contenuto effettivo della variazione né l'identificatore del soggetto cui questa si riferisce, poiché quest'ultimo è sostituito da un identificatore pseudonimizzato. Le informazioni aggiuntive per risolvere la pseudonimizzazione sono nella sola conoscenza del **Produttore** e da questa trasferita ai soli **Consumatori** che hanno un procedimento in essere per uno specifico soggetto.

La pseudonimizzazione dell'identificatore univoco del soggetto della variazione è ottenuta applicando una funzione di hashing con seme al fine di assicurare l'irreversibilità e l'univocità della pseudonimizzazione. Il **Produttore** DEVE comunicare ai **Consumatori**:

- l'algoritmo di hashing selezionato tra quelli dichiarati all'interno della cornice di sicurezza definita dal **MoDI** e riportati nell' ALLEGATO 4: PROCESSO DI DISTRIBUZIONE DEI SEGNALI DI VARIAZIONE;
- i parametri di esecuzione della funzione di hashing (per esempio il seme) così da consentire, a questi ultimi, il calcolo della pseudonimizzazione dei soggetti da lui conosciuti.

Tenuto conto della necessità di garantire che i **Segnali di Variazione** per dato un soggetto siano interpretabili solo dai **Consumatori** con un procedimento in essere sullo stesso e dato il carattere temporale tipicamente limitato di un procedimento, i **Produttori DEVONO** periodicamente modificare almeno uno dei parametri con cui attuano la pseudonimizzazione. A seguito della modifica dei suddetti parametri, tutti i nuovi **Segnali di Variazione** depositati presso l'**Infrastruttura interoperabilità PDND** riportano gli identificatori pseudonimizzati nuovi, al fine di rafforzare l'incapacità dei **Consumatori** di associare tali segnali a soggetti per cui non hanno procedimenti in essere. La periodicità della modifica dei parametri è definita dal **Produttore** e DEVE essere proporzionale alla tipologia di dati personali e alla riservatezza delle informazioni oggetto degli stati e dei fatti cui le variazioni possono riferirsi.

17. Scambio di dati/informazioni asincrono con callback

L'**Infrastruttura interoperabilità PDND** agevola la modalità di scambio di dati e informazioni asincrono con callback, quale applicazione del Pattern non bloccante RPC PUSH basato su callback, previsto nelle [LG INTEROPERABILITÀ TECNICA]. In base a tale modalità, lo scambio tra un **Erogatore** e un **Fruitore** è realizzato prevedendo i seguenti passi:

1. il **Fruitore** effettua una richiesta all'**Erogatore** includendo il riferimento al servizio di callback che dovrà essere invocato dall'**Erogatore** quando la risorsa predisposta dallo stesso in risposta alla richiesta del **Fruitore** è disponibile;
2. l'**Erogatore**, a valle della predisposizione della risorsa in risposta alla richiesta del **Fruitore** di cui al precedente passo 1, invocando il servizio di callback reso disponibile dal **Fruitore** può:
    a. inoltrare la risorsa al **Fruitore**, concludendo lo scambio;
    b. inoltrare il riferimento della risorsa al **Fruitore**;
3. Nel caso in cui l'**Erogatore** ha inoltrato il riferimento della risorsa al **Fruitore**, vedi precedente passo 2.b, lo stesso provvede a recuperare la risorsa indicata dall'**Erogatore**, concludendo lo scambio.

Gli standard e le tecnologie utilizzate applicati dall'**Infrastruttura interoperabilità PDND** e che DEVONO essere utilizzati dagli **Aderenti** per dare seguito allo scambio di dati/informazioni asincrono con callback sono oggetto dell'ALLEGATO 5: SCAMBIO DI DATI/INFORMAZIONI ASINCRONO CON CALLBACK.

L'**Infrastruttura interoperabilità PDND** rende disponibile agli **Aderenti** la possibilità di realizzare uno scambio di dati/informazioni asincrono con callback assicurando:

- all'**Erogatore** di registrare al momento della pubblicazione del proprio **e-service** le caratteristiche del servizio di callback che il **Fruitore** è tenuto ad implementare per la ricezione della risorsa o del riferimento alla risorsa;
- la gestione di **Voucher** dedicati alla presente fattispecie di interazione tra **Erogatore** e **Fruitore**, prevedendo in essi la registrazione delle informazioni per dare seguito ai passi dello scambio quali:
    - identificativo univoco dello scambio utilizzato dall'**Erogatore** e dal **Fruitore** per correlare i vari passi da loro eseguiti;
    - il riferimento al servizio di callback implementato dal **Fruitore** ed indicato dallo stesso per la ricezione della risorsa o del riferimento alla risorsa.

18. Disposizioni in materia di protezione dei dati personali

18.1. Ruolo dei soggetti coinvolti e trattamenti previsti

Ai sensi dell'articolo 50-ter, comma 6 del CAD, *"L'accesso ai dati attraverso la Piattaforma Digitale Nazionale Dati non modifica la disciplina relativa alla titolarità del trattamento, ferme restando le specifiche responsabilità ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 in capo al soggetto gestore della Piattaforma nonché le responsabilità dei soggetti accreditati che trattano i dati in qualità di titolari autonomi del trattamento"*.

Fatta eccezione per quanto attiene alle attività di cui all'allegato 4 e al ruolo svolto dal **Gestore** come meglio individuato nella valutazione di impatto per la protezione dei dati personali alla luce del contesto regolamentare e giurisprudenziale unionale in materia di protezione dei dati personali, la fruizione degli **e-service** non determina, sull'**Infrastruttura interoperabilità PDND**, alcun trattamento dei dati personali oggetto della trasmissione da **Erogatore** a **Fruitore**; ogni **Aderente** pertanto resta autonomo titolare del trattamento dei dati personali che rende disponibili o di cui fruisce nell'interazione con altro **Aderente** per mezzo dell'**Infrastruttura interoperabilità PDND**. Il **Gestore** agisce come titolare del trattamento per le attività necessarie all'implementazione e alla gestione dell'**Infrastruttura interoperabilità PDND**. Con riferimento ai trattamenti effettuati ai fini della distribuzione dei **Segnali di Variazione,** il **Gestore** assume il ruolo di responsabile del trattamento del **Produttore**.

Ogni **Aderente** che comunica dati personali si impegna a manlevare e tenere indenne il soggetto ricevente da ogni contestazione per i dati dallo stesso acquisiti in qualità di titolare del trattamento.

Ogni **Aderente** che riceve dati personali si impegna a manlevare e tenere indenne il soggetto da cui li ha ricevuti da ogni contestazione per i dati dallo stesso acquisiti in qualità di titolare del trattamento.

Resta fermo che, qualora un **Aderente,** agendo in qualità di **Delegato dell'Erogatore** o **del Fruitore**, tratti dati personali per conto della Pubblica Amministrazione delegante, questi svolge il ruolo di responsabile del trattamento ai sensi dell'articolo 4, paragrafo 1, numero 8) del GDPR per conto degli **Aderenti** che lo hanno nominato **Delegato dell'Erogatore o del Fruitore** e che **DEVONO**, pertanto, formalizzare prima che il trattamento abbia inizio**,** il suo ruolo ai sensi dell'articolo 28 del GDPR. Il **Gestore PUÒ** implementare una funzionalità volta alla stipula dell'atto giuridico concernente la nomina del **Delegato del Fruitore**.

Ruolo Aderente	**Ruoli GDPR**
Erogatore	Titolare del trattamento
Fruitore	Titolare del trattamento
Delegato dell'Erogatore	Responsabile del trattamento per conto dell'Erogatore
Delegato del Fruitore	Responsabile del trattamento per conto del Fruitore

Le attività di trattamento dei dati personali svolte dal **Gestore** a mezzo della **Infrastruttura interoperabilità PDND** sono le seguenti:

- accreditamento degli **Aderenti** e dei loro **Utenti degli Aderenti** e/o delegati;
- gestione delle attività connesse alla fruizione degli **e-service** e comunicazioni con gli **Aderenti** necessarie alla corretta gestione della **Infrastruttura interoperabilità PDND**;

- emissione dei **Voucher** su richiesta del **Fruitore**, in relazione ai dati personali di quest'ultimo o del suo operatore;
- attività di **Auditing** di cui al precedente CAPITOLO 13;
- attività di **Tracing** di cui al precedente CAPITOLO 13;
- attività di anonimizzazione e/o aggregazione sulla totalità dei dati acquisiti;
- monitoraggio del funzionamento e utilizzo dell'**Infrastruttura interoperabilità PDND** e di miglioramento ed evoluzione della stessa (analisi, ricerca e sviluppo).

In ognuna di tali attività, il **Gestore DEVE** assicurare la protezione dei dati personali trattati, nel rispetto della normativa nazionale e unionale.

Atteso che sull'**Infrastruttura interoperabilità PDND** le uniche attività che comportano il trattamento di dati personali sono poste in atto dal **Gestore**, nei seguenti paragrafi sono individuate specifiche disposizioni in merito alla protezione dei dati personali rivolte al **Gestore** nell'implementazione e nella gestione dell'**Infrastruttura interoperabilità PDND**, oltre ad alcune indicazioni rivolte agli **Aderenti**, seppur relative ad attività esterne all'**Infrastruttura interoperabilità PDND**.

Resta fermo in ogni caso che qualsiasi **Aderente**, sia in qualità di **Erogatore** sia di **Fruitore**, nella predisposizione dei propri sistemi informatici per l'utilizzo della **PDND** e per l'erogazione e la fruizione delle API, DEVE operare in conformità alla normativa unionale e nazionale vigente in tema di protezione dei dati personali, fra cui i provvedimenti del Garante per la protezione dei dati personali in materia di misure di sicurezza e modalità di scambio dei dati, e nel rispetto della continuità di servizio.

18.2. Necessità e proporzionalità del trattamento

18.2.1. Minimizzazione

Il **Gestore** DEVE ridurre il trattamento ai soli dati personali strettamente necessari per il perseguimento delle finalità poste alla base delle singole attività di trattamento e, conseguentemente, essere in grado di comprovare, nel rispetto del principio di responsabilizzazione, che i dati personali siano pertinenti, necessari e non eccessivi rispetto alla finalità perseguita.

A tal fine il **Gestore** DEVE effettuare una ricognizione dei dati personali il cui trattamento risulta necessario e individuare le categorie dei dati personali e degli interessati coinvolti, la finalità per cui sono trattati i dati e la base giuridica del loro trattamento.

18.2.2. Limitazione dei tempi di conservazione

Il **Gestore** DEVE conservare documenti e informazioni per il tempo strettamente necessario, al fine di garantire il rispetto del principio di limitazione della conservazione e per ridurre l'impatto dei rischi gravanti sui diritti e le libertà degli interessati. I tempi di conservazione sono i seguenti:

a. con riferimento all'**Accordo di Adesione**: 10 anni decorrenti dalla cessazione del rapporto contrattuale;
b. con riferimento alle registrazioni degli **e-service**: 10 anni decorrenti dalla cancellazione dell'API dell'e-service dal **Catalogo API**;
c. con riferimento agli **Attributi degli Aderenti**: 10 anni decorrenti dalla cancellazione dell'attributo;
d. con riferimento alle attività di tracciamento dei log di sistema: 24 mesi decorrenti dalla registrazione del log;
e. con riferimento alle risultanze dell'**Auditing**: 10 anni decorrenti dalla memorizzazione;
f. con riferimento alle risultanze del **Tracing**: 12 mesi decorrenti dalla memorizzazione.

Il **Gestore** DEVE:

a. implementare misure tecniche e/o organizzative che consentano di rilevare la scadenza del periodo di conservazione;
b. implementare misure tecniche e/o organizzative che consentano la cancellazione dei dati personali alla scadenza del periodo di conservazione e assicurarsi che il metodo scelto per l'eliminazione sia appropriato rispetto ai rischi legati ai diritti e alle libertà dei soggetti interessati;
c. eliminare i dati personali quando il periodo di conservazione definito nella relativa procedura scade.

18.3. Misure di responsabilizzazione

Il **Gestore** DEVE predisporre una valutazione di impatto sulla protezione dei dati personali ai sensi dell'articolo 35 del GDPR, anche alla luce del paragrafo 10 della medesima disposizione, che indichi anche le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nonché a tutela dei diritti e delle libertà degli interessati, con riferimento ai trattamenti effettuati nell'ambito dell'**Infrastruttura interoperabilità PDND**.

Tale valutazione d'impatto è messa a disposizione di tutti i soggetti **Aderenti**.

Qualora il trattamento di dati personali scaturente dalla predisposizione dell'**e-service** non sia già stato effettuato in differente modalità al di fuori dell'**Infrastruttura interoperabilità PDND**, altresì l'Erogatore e il **Fruitore** DEVONO effettuare la valutazione d'impatto sulla protezione dei dati personali ai sensi dell'articolo 35 del GDPR e annotare il relativo trattamento all'interno del proprio Registro delle attività di trattamento ai sensi dell'art. 30 del GDPR.

18.4. Trasparenza e rispetto dell'esercizio dei diritti degli utenti

Per quanto concerne i trattamenti la cui titolarità è individuata in capo al **Gestore**, questi DEVE rendere, mediante l'**Infrastruttura interoperabilità PDND**, un'apposita informativa ai sensi degli articoli 12, 13 e 14 del GDPR.

Il **Gestore** DEVE adottare misure organizzative adeguate a garantire l'esercizio dei diritti degli interessati.

18.4.1. Responsabili del trattamento e trasferimenti di dati personali

Nell'erogazione dei servizi e delle funzionalità previste dall'**Infrastruttura interoperabilità PDND**, il **Gestore** PUÒ fare ricorso a soggetti terzi, opportunamente nominati responsabili del trattamento secondo le modalità stabilite all'articolo 28 del GDPR.

In tal caso, il **Gestore** DEVE privilegiare fornitori situati sul territorio nazionale e dell'Unione Europea. Laddove non sia possibile, il **Gestore** PUÒ ricorrere a responsabili situati in Paesi terzi, che offrano garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate alla sicurezza dei trattamenti e alla tutela dell'interessato, ponendo in tal caso una particolare attenzione all'adozione di misure tecniche e organizzative adeguate a impedire trattamenti avulsi dalle finalità del trattamento e a evitare che terzi non autorizzati possano accedere ai dati personali, tenuto conto - ai sensi dell'articolo 32 del GDPR - dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

In ogni caso, laddove possibile, il **Gestore DEVE** istruire i responsabili del trattamento sulla necessità di conservare i dati personali all'interno dell'Unione Europea.

Il **Gestore DEVE**, in ogni caso, rispettare le misure previste dal Capo V del GDPR.

18.4.2. Sicurezza del trattamento

Ai sensi del Considerando 83 e dell'articolo 32 del GDPR e nel rispetto del principio di responsabilizzazione, il **Gestore DEVE** implementare ogni misura tecnica e organizzativa adeguata a garantire un livello di sicurezza adeguato al rischio.

Tali misure di sicurezza comprendono almeno:

a. la cifratura "in transit" e "data at rest" e la anonimizzazione;
b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d. prevedere all'interno dei processi condivisi un momento dedicato a verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Di seguito si evidenziano le *best practice* in tema di sicurezza del trattamento dei dati personali con riferimento al contesto oggetto delle presenti Linee guida.

18.4.2.1. Cifratura dei dati personali

Il **Gestore** DEVE trattare i dati implementando misure in grado di rendere incomprensibili i dati personali a chiunque non sia autorizzato ad accedervi:

a. determinando le componenti critiche su cui applicare misure di crittografia ("at rest", es: dischi rigidi, file, ecc.; "in transit", es: trasferimento da/verso un database, canali di comunicazione) in base a:
   i. forma/posizione in cui sono memorizzati/resi disponibili i dati personali;
   ii. rischi individuati;
   iii. prestazioni richieste;
b. scegliendo il tipo di crittografia (simmetrica o asimmetrica) in base al contesto e ai rischi individuati;
c. adottando soluzioni di crittografia basate su algoritmi pubblici notoriamente forti;
d. definendo ulteriori misure per garantire la disponibilità, l'integrità e la riservatezza delle informazioni.

18.4.2.2. Anonimizzazione dei dati personali

Laddove possibile, il **Gestore DEVE** eliminare le caratteristiche che consentono di identificare direttamente l'interessato. In particolare, **DEVE**:

a. determinare ciò che deve essere reso anonimo in base al contesto, alla forma in cui vengono memorizzati i dati personali (compresi i campi del database o estratti dai testi) e ai rischi individuati;
b. scegliere strumenti (inclusi, l'hashing e la tokenizzazione) che rispondano innanzitutto alle esigenze funzionali.