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 CAD

Versione 1.0 del 10.12.2021

1 Introduzione 5
2 Riferimenti e sigle 7
2.1 Note di lettura del documento 7
2.2 Struttura 7
2.3 Riferimenti Normativi 8
2.4 Linee guida di primario riferimento 9
2.5 Acronimi 9
3 Ambito di applicazione 10
3.1 Soggetti destinatari 10
3.1.1 Soggetti erogatori 10
3.1.2 Soggetti fruitori 10
3.1.3 Gestore 11
4 Definizioni 12
4.1 Aderente 12
4.2 Accordo di Adesione 12
4.3 Erogatore 12
4.4 Fruitore 12
4.5 Attributi degli Aderenti 12

4.6 Registro degli Attributi 13
4.7 Utenti degli Aderenti 13
4.8 Capofila 13
4.9 API 14
4.10 Template e-service 14
4.11 E-service 15
4.12 Catalogo API 15
4.13 Requisiti di Fruizione 16
4.14 Voucher 16
4.15 Pattern di interazione 16
4.16 Pattern di sicurezza 16
4.17 Profili di interoperabilità 17
4.18 Service Level Agreements (SLA) 17
5 Adesione 18
6 Gestione degli Attributi degli Aderenti 20
7 Catalogo API 24
8 Richiesta di fruizione dell'e-service 27
9 Analisi del rischio sulla protezione dei dati personali e configurazione del servizio di erogazione 28
10 Responsabilità 31

11 Trust Infrastruttura interoperabilità PDND e sistemi informatici degli Aderenti 35

12 Raccolta delle informazioni relative agli accessi e alle transazioni 37

13 Livelli di servizio dell'Infrastruttura interoperabilità PDND 39

13.1 Indicatori dei servizi/API realizzati 39

13.1.1 Tempo di risposta delle richieste su percentile 39

13.1.2 Numero di richieste per unità di tempo 40

13.1.3 Numero di richieste con risposta di errore per unità di tempo 40

13.2 Indicatori dei servizi di supporto 41

13.2.1 Tempestività di ripristino dell'operatività 41

13.2.2 Tempestività di risposta a segnalazioni di anomalie 41

14 Disposizioni in materia di protezione dei dati personali 42

14.1 Ruolo dei soggetti coinvolti e trattamenti previsti 42

14.2 Necessità e proporzionalità del trattamento 44

14.2.1 Minimizzazione 44

14.2.2 Limitazione dei tempi di conservazione 44

14.3 Misure di responsabilizzazione 45

14.4 Trasparenza e rispetto dell'esercizio dei diritti degli utenti 45

14.4.1 Responsabili del trattamento e trasferimenti di dati personali 46

14.4.2 Sicurezza del trattamento 46

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 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 disciplina 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 per il tramite dell'**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 3 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

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".

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 PA, 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
[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
[SLA]	Service Level Agreement, ovvero accordo sul livello di servizio frutto della contrattazione tra erogatore e fruitore

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, i quali, 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 nonché la condivisione dei dati 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, assicurando le modalità di scambio telematico per il tramite di **API** come previsto dal **MoDI**.

In particolare, i soggetti di cui all'articolo 2, comma 2, del CAD attuano le **Linee Guida** al fine di condividere i dati e le informazioni da essi detenuti, 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**.

In tale contesto, i soggetti di cui all'art. 2, comma 2, del CAD agiscono in veste di soggetti erogatori.

3.1.2 Soggetti fruitori

Le Linee Guida sono rivolte, altresì, ai soggetti privati che, unitamente ai citati soggetti di cui all'art. 2, comma 2, del CAD, siano stati abilitati a fruire della **PDND** al fine di accedere ai dati e alle informazioni ivi resi disponibili.

In tale contesto, i soggetti di cui all'art. 2, comma 2 del CAD e i soggetti privati agiscono in qualità di soggetti fruitori.

Si ricorda che l'art. 50, comma 2 del CAD stabilisce che "Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive".

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 "5 Adesione") per erogare e/o usufruire di servizi mediante le funzionalità dell'infrastruttura.

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 in proprio possesso o per l'integrazione di processi.

4.4 Fruitore

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

4.5 Attributi degli Aderenti

Sono le caratteristiche dell'**Aderente**, disciplinate nel capitolo "6 Gestione degli Attributi degli Aderenti".

4.6 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.

4.7 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.

4.8 Capofila

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 **Erogatrice** a utilizzare per suo conto le funzionalità dell'infrastruttura medesima per la registrazione e la modifica degli **e-service** sul **Catalogo API.**

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

Le pubbliche amministrazioni **Erogatrici** POSSONO delegare una o più **Capofila** tra quelle che si sono candidate a tal fine sull'**Infrastruttura interoperabilità PDND**.

La delega alla **Capofila** ha effetto al momento dell'accettazione di quest'ultima e determina la possibilità, per i suoi **Utenti degli Aderenti**, di operare sulla **Infrastruttura interoperabilità PDND** per conto dell'**Erogatrice** delegante.

4.9 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.

4.10 Template e-service

L'**Infrastruttura interoperabilità PDND** favorisce i processi di co-design individuati nella governance della trasformazione del Piano Triennale per l'informatica nella Pubblica Amministrazione, tramite il meccanismo dei template.

Per **Template e-service** si intende la definizione di un modello di descrittori 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 a cui gli **Aderenti** POSSONO attenersi durante il processo di implementazione.

Il **Template e-service** descrive quindi come un **e-service** DEVE erogare il servizio non entrando nel merito di come verrà implementato né indicando le tecnologie adottate per l'implementazione delle logiche di business.

Solo dopo il processo di implementazione del **Template e-service** si avranno una o più istanze di un **e-service** reale pronto alla pubblicazione sul **Catalogo API**.

Il co-design coinvolge:

- **API Co-design Manager**: è un **Aderente**, che all'interno del gruppo di Pubbliche Amministrazioni interessate al co-design di un **e-service**, disegna e registra il **Template e-service** sull'Infrastruttura interoperabilità PDND provvedendo a:
  - dichiarare, nel rispetto del **MoDI**, il **Template e-service** delle API che implementa l'**e-service**;
  - definire quali informazioni sono necessarie per implementare il **Template** e renderlo operativo, in questa maniera vengono definiti i margini di libertà entro i quali può agire chi vuole implementare l'**e-service**.

- **Implementatore**: è un **Aderente** che decide di implementare l'**e-service** descritto da un **Template e-service** e provvede a:
  - compilare il **Template e-service** definito dal **API Co-design manager** nel rispetto dei margini di libertà previsti;
  - prendersi carico dell'implementazione dell'istanza dell'**e-service**.

L'**Infrastruttura interoperabilità PDND** permette la ricerca e l'identificazione dei **Template e-service** registrati dagli **API Co-design manager**.

L'**Infrastruttura interoperabilità PDND** promuove e comunica la pubblicazione di nuove versioni di **Template e-service** e supporta la pubblicazione sul **Catalogo API** delle istanze implementate dagli **Aderenti**.

4.11 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 dati e/o l'integrazione di processi.

4.12 Catalogo API

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.

È realizzato dall'**Infrastruttura interoperabilità PDND**.

4.13 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**.

4.14 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**.

4.15 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**.

4.16 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.).

4.17 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**.

4.18 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.**

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**.

5 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:
   - soggetto **Aderente**, qualora si tratti di persona fisica;
   - del rappresentante legale o di un suo delegato, qualora l'**Aderente** sia una persona giuridica;
2. qualificazione del soggetto **Aderente** come pubblica amministrazione, gestore di pubblico servizio o società a controllo pubblico - ai sensi dell'articolo 2, comma 2 del **CAD** - oppure come soggetto privato;
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**, preventivamente sottoscritto dal **Gestore**, 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:

- nei confronti dei soggetti di cui all'articolo 2, comma 2 del CAD l'abilitazione all'utilizzo delle funzionalità previste per i ruoli di **Erogatore** e di **Fruitore**;
- nei confronti dei soggetti privati l'abilitazione all'utilizzo delle sole funzionalità previste per il ruolo di **Fruitore**;
- 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** DEVE periodicamente verificare le condizioni che hanno determinato l'adesione dei soggetti interessati.

6 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**.

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:

1. 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** 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;
2. 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.

In merito agli **Attributi Verificati** si precisa che:

1. un **Fruitore** NON DOVREBBE chiedere la verifica di un attributo **Verificato** che sia stato precedentemente rifiutato da un **Erogatore**, a meno che siano mutate le condizioni che ne determinano il possesso;
2. un **Erogatore** PUÒ definire il periodo temporale di validità di un attributo **Verificato** ai fini della fruizione dei propri **e-service**, scaduto il quale l'attributo dovrà essere verificato nuovamente. Alla scadenza, qualora l'**Erogatore** non provveda a una nuova verifica, l'**infrastruttura Interoperabilità PDND** sospende l'emissione dei **Voucher** per gli **e-service** per cui i relativi **Requisiti di Fruizione** risultano non più soddisfatti, assumendo l'attributo **Verificato** non soddisfatto. Nel caso in cui la natura dell'**Attributo Verificato** ne evidenzi la possibilità di variazioni nel tempo, l'**Erogatore** DEVE definire il periodo temporale di validità;
3. un **Erogatore PUÒ** ritenere valida - assumendosene la responsabilità - la verifica di un attributo effettuata da altro **Erogatore**, in considerazione della natura di quest'ultimo, nonché delle caratteristiche anche temporali dell'attributo;
4. nel caso in cui l'esito della verifica effettuata da un **Erogatore** contrasti con quanto precedentemente constatato da un altro **Erogatore**, l'**Infrastruttura interoperabilità PDND** comunica tale circostanza agli **Erogatori** interessati, invitandoli a dirimere l'ambiguità e a segnalare l'eventuale volontà di sospendere la fruizione dell'**e-service** da parte del **Fruitore** il cui attributo è stato oggetto di verifica con risultato contrastante.

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 5, 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** sono inseriti nel **Registro degli Attributi** a cura degli **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 predetta 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 ad aggiornare l'associazione tra gli **Aderenti** e gli **Attributi Certificati** in relazione alle variazioni delle banche dati individuate in conformità a quanto indicato alla precedente lettera a).

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**.

7 Catalogo API

Il **MoDI** individua nelle [LG INTEROPERABILITÀ TECNICA] il **Catalogo delle 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.

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 dalle [LG INTEROPERABILITÀ TECNICA], per usufruire dell'**e-service**;
- la documentazione accessoria e manualistica per l'utilizzo del **e-service**.

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 **Capofila**.

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].

Nell'implementazione dei propri **e-service** al di fuori dell'**Infrastruttura interoperabilità PDND**, gli **Erogatori** DEVONO prevedere un campo per l'indicazione da parte dei **Fruitori** del riferimento ai documenti informatici che possano provare la legittimità 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 compilare il suddetto riferimento sotto la propria responsabilità;
- l'**Erogatore** NON DEVE dare seguito alla richiesta del **Fruitore** in assenza del suddetto riferimento.

La raccolta e la memorizzazione di tali riferimenti non avviene sulla **Infrastruttura interoperabilità PDND.**

Nel caso in cui il **Fruitore** sia un soggetto privato, lo stesso DEVE permettere agli **Erogatori** di recuperare i documenti che attestino la legittimità 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 legittimità 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**.

8 Richiesta di fruizione dell'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**. Tale verifica PUO' non essere espletata qualora sussistano entrambe le seguenti ipotesi:
    - la verifica sia stata già positivamente espletata da altro **Erogatore;**
    - l'**Erogatore** interessato, in sede di definizione dei **Requisiti di Fruizione** dell'**e-service**, avesse dichiarato di accettare le verifiche realizzate da altri **Erogatori**.

L'**Infrastruttura interoperabilità PDND** DEVE rendere disponibili agli **Aderenti** le funzionalità per attuare i passaggi indicati in precedenza.

La richiesta di fruizione di un **e-service** è conclusa con esito positivo se risulta soddisfatta una delle seguenti condizioni:

- all'**Aderente** sono associati **Attributi certificati** tali da soddisfare i **Requisiti di Fruizione** stabiliti dall'**Erogatore** per lo specifico **e-service**;
- l'**Aderente** ha dichiarato **Attributi dichiarati**, cosi 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**;
- l'**Aderente** ha dichiarato **Attributi verificati**, cosi come indicato al precedente passaggio 1, e gli stessi sono stati verificati dall'**Erogatore** dell'e-service, cosi 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.**

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**.

9 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**, cosi come indicato al precedente capitolo 8 Richiesta di fruizione dell'e-service**,** il **Fruitore** DEVE, nei casi diversi dagli **e-service** che rendono disponibili dati aperti ai sensi Direttiva (UE) 2019/1024, 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 al trattamento derivante dalla fruizione dell'**e-service**.

Il **Fruitore** effettuare un'analisi del rischio per ogni finalità di fruizione dell'**e-service**.

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'effettuazione dell'analisi del rischio sulla protezione dei dati personali e del l'indicazione della stima di carico, l'**Infrastruttura interoperabilità PDND**, nell'ipotesi in cui la richiesta del **Fruitore** ecceda la disponibilità 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**. 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, PUO':

- sospendere o eliminare una finalità precedentemente registrata sulla **Infrastruttura interoperabilità PDND**;
- ridurre l'indicazione della stima di carico di una specifica finalità precedentemente registrata sulla **Infrastruttura interoperabilità PDND**;
- 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 di 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** NON DEVE emettere **Voucher** per singola finalità di fruizione sospesa o bloccata dagli **Aderenti**.

10 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) 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 tempestivamente gli **Aderenti** interessati in caso di violazioni di sicurezza o di qualsiasi minaccia che comporti, nell'ambito del complessivo utilizzo della **Infrastruttura interoperabilità PDND**, un rischio per la sicurezza e per i diritti e le libertà degli interessati e stabilendone le modalità all'interno della valutazione d'impatto sulla protezione dei dati personali;
c) in caso di violazione dei dati personali, procedere all'eventuale notifica al Garante per la protezione dei dati personali e, ove necessario, alla comunicazione agli interessati in applicazione degli artt. 33 e 34 del GDPR.

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 sin dalla progettazione e per impostazione predefinita, effettuando un'analisi del rischio 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 che abbia compilato l'Analisi del rischio;

c) la minimizzazione, l'esattezza, l'integrità e la riservatezza dei dati comunicati al **Fruitore** in fase di erogazione dell'e-service;
d) 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;
e) 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 il **Gestore** e 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;
f) in caso di violazione dei dati personali, l'eventuale notifica al Garante per la protezione dei dati personali e, ove necessario, la comunicazione agli interessati in applicazione degli artt. 33 e 34 del GDPR;
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) effettuare l'analisi del rischio sulla protezione dei dati personali che saranno ottenuti mediante 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) comunicare direttamente all'**Erogatore** il riferimento ai documenti informatici 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**;

d) 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 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;
e) 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**;
f) individuare, all'interno della propria organizzazione e accreditare sulla **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;
g) comunicare tempestivamente all'**Erogatore** eventuali sopravvenute criticità che impattino sulla fruizione dell'**e-service;**
h) comunicare immediatamente all'**Erogatore** il verificarsi di eventi che impattino sulla sicurezza della fruizione dell'**e-service**;
i) segnalare immediatamente all'**Erogatore** qualsiasi malfunzionamento o disservizio riscontrato in fase di accesso e/o fruizione dell'**e-service**;
j) in caso di violazione dei dati personali, procedere all'eventuale notifica al Garante per la protezione dei dati personali e, ove necessario, alla comunicazione agli interessati in applicazione degli artt. 33 e 34 del GDPR;
k) 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 il **Gestore** e 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;
l) dotarsi degli strumenti e di tutte le soluzioni informatiche necessarie a un uso ottimale delle funzionalità di fruizione dell'**e-service**;
m) 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**;

n) 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**.

11 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 materiale crittografico utilizzato dagli **Aderenti** per verificare i **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 infrastruttura.

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**, 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.

12 Raccolta delle informazioni relative agli accessi e alle transazioni

L'**Infrastruttura interoperabilità PDND** fornisce il 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 alcuna verifica in merito agli 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 nel tempo della disponibilità delle API presenti nel relativo Catalogo e dichiarate "in erogazione". L'**Erogatore** deve includere nella firma dell'**e-service** una chiamata secondo le indicazioni presenti nella documentazione tecnica caricata sul portale della **Infrastruttura interoperabilità PDND**. L'**Infrastruttura Interoperabilità PDND** conserva, anche in maniera aggregata, gli esiti delle chiamate in termini di:
    - successo/fallimento;
    - coordinate temporali;
    - tempi di risposta.
- Auditing: registrazione delle autorizzazioni (Voucher) rilasciate dalla **Infrastruttura Interoperabilità PDND** e richieste dai **Fruitori**. L'**Infrastruttura interoperabilità** conserva 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.

Il **Gestore** dell'**Infrastruttura interoperabilità PDND** PUÒ implementare anche un servizio di Tracing, ossia un servizio di raccolta dei tracciati che descrivono l'andamento esclusivamente quantitativo delle transazioni avvenute tra ciascun **Erogatore** e ciascun **Fruitore**. Le informazioni raccolte mediante tale servizio - che non dovranno comprendere il contenuto informativo scambiato tra **Erogatore** e **Fruitore** - descriveranno il numero di transazioni intervenute tra **Erogatore** e **Fruitore** in un determinato arco di tempo.

In caso di implementazione di tale servizio, il **Gestore** informa gli **Aderenti** con il preavviso indicato nella **Accordo di Adesione.**

In tal caso, gli **Aderenti** DEVONO depositare, con le modalità e le tempistiche che saranno indicate nella **Accordo di Adesione**, sulla **Infrastruttura interoperabilità PDND** i tracciati delle transazioni a cui hanno partecipato in qualità sia di **Erogatore** sia di **Fruitore**.

Le informazioni depositate dagli **Aderenti** sull'**Infrastruttura interoperabilità PDND** DEVONO essere aggregate in base ai seguenti criteri:

- coordinate temporali con la granularità che sarà definita;
- **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 **Aderenti** 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.

13 Livelli di servizio dell'Infrastruttura interoperabilità PDND

Il rapporto tra il **Gestore** e gli **Aderenti** è regolato dai livelli di qualità, oggetto dell'Allegato della **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 della **Accordo di Adesione**.

13.1 Indicatori dei servizi/API realizzati

13.1.1 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 nella **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**.

13.1.2 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 nella **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 rappresentato dai log file tenuti dall'**Infrastruttura interoperabilità PDND**.

13.1.3 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 della 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 nella **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 rappresentato dai log file tenuti dalla **Infrastruttura interoperabilità PDND**.

13.2 Indicatori dei servizi di supporto

13.2.1 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**

13.2.2 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 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**.

14 Disposizioni in materia di protezione dei dati personali

14.1 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*".

Premesso che 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** 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**.

Resta fermo che, qualora un **Aderente** agisca in qualità di **Capofila**, 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 **Capofila** e che DEVONO, pertanto, formalizzare preventivamente 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 dei **Capofila** quali responsabili del trattamento.

Nel ribadire che la fruizione degli **e-service** non determina, sull'**Infrastruttura interoperabilità PDND**, alcun trattamento dei dati personali oggetto della trasmissione da **Erogatore** a **Fruitore,** il **Gestore** agisce come titolare del trattamento per le attività necessarie all'implementazione e alla gestione dell'**Infrastruttura interoperabilità PDND** e non necessita, pertanto, di alcuna nomina ai sensi dell'28 del GDPR da parte degli **Aderenti**.

Le predette attività di trattamento dei dati personali svolte dal **Gestore**, in qualità di titolare del trattamento, 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 dell'**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 10;
- attività di Tracing di cui al precedente capitolo 10;
- 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 **Erogatori**, 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, nonché dei 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.

14.2 Necessità e proporzionalità del trattamento

14.2.1 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.

14.2.2 Limitazione dei tempi di conservazione

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

a. con riferimento alle **Lettere 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.

14.3 Misure di responsabilizzazione

Il **Gestore** DEVE predisporre una valutazione di impatto sulla protezione dei dati personali e consultare il Garante per la protezione dei dati personali ai sensi degli articoli 35 e 36 del GDPR.

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** DEVE 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.

14.4 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.

14.4.1 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.

Il **Gestore** DEVE istruire i responsabili del trattamento sulla necessità di conservare i dati personali all'interno dell'Unione Europea laddove i fornitori non siano in grado di offrire garanzie sufficienti ad assicurare l'effettivo rispetto del Capo V del GDPR relativamente alle misure tecniche e organizzative adeguate alla sicurezza dei trattamenti e alla tutela dell'interessato.

14.4.2 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 l'anonimizzazione dei dati personali;
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 practices*" in tema di sicurezza del trattamento dei dati personali con riferimento al contesto oggetto delle presenti Linee guida.

14.4.2.1 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.

14.4.2.2 Anonimizzazione dei dati personali

Laddove possibile, il **Gestore** DEVE eliminare le caratteristiche che identificano i dati personali. In particolare DEVE:

a. determinare ciò che deve essere 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. anonimizzare permanentemente i dati che richiedono tale criterio di protezione in base alla forma dei dati (inclusi database e record testuali) e ai rischi individuati;

c. se i dati non possono essere anonimizzati in modo permanente, scegliere strumenti (inclusi la cancellazione parziale, la cancellazione, la ricerca di *hashing* e l'indice) che rispondano innanzitutto alle esigenze funzionali.