AGID | Agenzia per l'Italia Digitale

Linee guida sul punto di accesso telematico ai servizi della Pubblica Amministrazione

Articolo 64-bis del Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.

Versione 1 del 3 novembre 2021

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Sommario

Introduzione

L'art. 64-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82, s.m.i., recante il "Codice dell'amministrazione digitale" (nel seguito anche "**CAD**"), prevede che "*i soggetti di cui all'articolo 2, comma 2, rendono fruibili i propri servizi in rete, in conformità alle Linee guida, tramite il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri* […]".

Ai sensi dell'art. 64-bis, comma 1-bis, "[…] *i soggetti di cui all'art. 2, comma 2, i fornitori di identità digitali e i prestatori di servizi fiduciari qualificati, in sede di evoluzione, progettano e sviluppano i propri sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi e con i servizi di cui ai commi 1 e 1 ter, espongono per ogni servizio le interfacce applicative* […]".

Le attività di progettazione, sviluppo, gestione e implementazione del Punto di accesso telematico attivato presso la Presidenza del Consiglio dei Ministri sono attribuite alla Società PagoPA S.p.A. (di seguito "**Gestore**"), ai sensi dell'art. 8 del decreto legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla legge 11 febbraio 2019, n. 12.

Le presenti linee guida (di seguito "**Linee guida**"), relativamente al Punto di accesso telematico di cui all'articolo 64-bis del CAD, individuano:

- i principi adottati dal Gestore e dai soggetti di cui all'art. 2, comma 2 del CAD o da altri soggetti che rendono fruibili uno o più servizi tramite il Punto di accesso telematico per la realizzazione dei servizi in rete per il tramite del Punto di accesso telematico;
- l'architettura logica del Punto di accesso telematico e l'insieme di funzionalità implementate dal Punto di accesso telematico per dare seguito alla realizzazione dei Servizi in rete per il suo tramite;
- le integrazioni realizzate dal Punto di accesso telematico con le piattaforme previste dal CAD detenute dai soggetti di cui all'art. 2, comma 2, dai gestori di identità digitali e dai prestatori di servizi fiduciari qualificati;
- il modello di *governance* del Punto di accesso telematico che il Gestore applica per soddisfare le esigenze espresse dai Soggetti erogatori in merito alla realizzazione e messa in esercizio dei Servizi in rete per il tramite del Punto di accesso telematico;

- le disposizioni in materia di sicurezza e protezione dei dati personali che il Gestore e i Soggetti erogatori assicurano nella realizzazione e messa in esercizio dei Servizi in rete per il tramite del Punto di accesso telematico.

Il Gestore e i Soggetti erogatori nella realizzazione e messa in esercizio del Punto di accesso telematico e dei servizi in rete realizzati o resi fruibili per il suo tramite e, nondimeno, i soggetti di cui all'art. 2, comma 2, i gestori di identità digitali e i prestatori di servizi fiduciari qualificati relativamente all'integrazione delle piattaforme previste dal CAD con il Punto di accesso telematico assicurano l'attuazione delle presenti Linee guida e, in generale, delle linee guida emanate ai sensi dell'articolo 71 del CAD.

Capitolo 1

Ambito di applicazione

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

1.1 Soggetti destinatari

Come indicato all'articolo 64-bis, comma 1 del CAD, le presenti Linee guida sono destinate ai soggetti di cui all'articolo 2, comma 2 del CAD, che le attuano per rendere fruibili i propri servizi in rete per il tramite del Punto di accesso telematico di cui al medesimo articolo 64-bis del CAD.

Le Linee guida sono altresì destinate ai gestori di identità digitali e ai prestatori di servizi fiduciari qualificati, ai sensi dell'art. 64-bis, comma 1-bis del CAD.

Le Linee guida, infine, sono altresì rivolte PagoPA S.p.A., che le attua in merito alla progettazione, allo sviluppo e alla gestione del Punto di accesso telematico attivato presso la Presidenza del Consiglio dei Ministri.

Capitolo 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» e «OPZIONALE», la cui interpretazione è descritta di seguito.

- DEVE o DEVONO, indicano un requisito obbligatorio per rispettare la Linee guida;
- NON DEVE o NON DEVONO, 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 o restrizione la specifica.

2.2 Struttura

Le presenti Linee guida includono i seguenti allegati:

- Allegato 1: Procedura per l'adesione dei Soggetti erogatori al Punto di accesso telematico
- Allegato 2: Funzionalità del Punto di accesso telematico
- Allegato 3: Integrazione del Punto di accesso telematico con le piattaforme digitali previste dal CAD e normative specifiche
- Allegato 4: Domain model del Punto di accesso telematico
- Allegato 5: Misure minime di sicurezza

Al fine di assicurare l'allineamento costante delle Linee guida alle continue evoluzioni tecnologiche, l'aggiornamento degli allegati contenenti specifiche tecniche già disciplinate da norme, è realizzato attraverso atti emanati dall'AgID anche su proposta motivata del Gestore.

2.3 Riferimenti Normativi

Sono riportati di seguito gli atti normativi di riferimento del presente documento.

[D.Lgs. 82/2005]	Decreto legislativo 7 marzo 2005, n. 82 recante "Codice dell'amministrazione digitale";
[CE 2008/1205]	Regolamento (CE) n. 1205/2008 della Commissione del 3 dicembre 2008 recante attuazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda i metadati;
[D.Lgs. 196/2003]	Decreto legislativo 30 giugno 2003, n. 196 e s.m.i., recante Codice in materia di protezione dei dati personali (di seguito "**Codice Privacy**")
[UE 679/2016]	Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito "**GDPR**")
[UE 910/2014]	Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (di seguito "**eIDAS**")
[D.L. 135/2018]	Decreto-legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla Legge 11 febbraio 2019, n. 12;
[DPCM 24/10/2014]	Decreto del Presidente del Consiglio dei Ministri del 24 ottobre 2014 recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese";
[AgID 44/2015]	Determinazione dell'Agenzia per l'Italia Digitale n. 44 del 28 luglio 2015 recante regolamenti SPID;
[AgID 189/2016]	Determinazione dell'Agenzia per l'Italia Digitale n. 189 del 22 luglio 2016 recante modifiche regolamenti SPID;
[D. Interno 23/12/2015]	Decreto del Ministero dell'Interno 23 dicembre 2015 recante "Modalità tecniche di emissione della Carta d'identità elettronica";
[Legge 4/2004]	Legge 9 gennaio 2004, n. 4 e sm.i., recante "Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici";
[D.Lgs. 106/2018]	Decreto legislativo 10 agosto 2018, n. 106 recante "Riforma dell'attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici";

[Legge 241/1990]	Legge 7 agosto 1990, n. 241 e s.m.i. recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
[D.P.R. 445/2000]	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i., recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa".

2.4 Linee guida di riferimento

Di seguito sono elencate le linee guida emesse dall'AgID ai sensi dell'articolo 71 del CAD che sono richiamate nel presente documento.

[LG DESIGN]	Linee guida di design per i servizi della pubblica amministrazione
[LG PAGOPA]	Linee guida per l'Effettuazione dei Pagamenti Elettronici a favore delle Pubbliche Amministrazioni e dei Gestori di Pubblici Servizi
[LG ACCESSIBILITÀ]	Linee guida sull'accessibilità degli strumenti informatici
[LG RECOVERY]	Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni
[LG OPEN SOURCE]	Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni
[LG IPA]	Linee guida dell'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi
[LG INAD]	Linee guida dell'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
[LG PDND]	Linee guida infrastruttura tecnologica per l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici
[LG INTEROP TEC]	Linee guida sull'interoperabilità tecnica
[LG SICUREZZA]	Linee guida sulla sicurezza ICT
[LG SVILUPPO]	Linee guida per lo sviluppo del software sicuro

2.5 Termini e definizioni

Di seguito si riportano i termini e le definizioni che vengono utilizzati nelle presenti Linee guida:

[Punto di accesso telematico]	L'insieme dei sistemi e delle componenti tecnologiche realizzate dal Gestore per l'accesso telematico ai servizi della Pubblica Amministrazione ai sensi dell'art. 64-bis del CAD
[App IO]	L'applicazione mobile per l'accesso ai Servizi messi a disposizione dai Soggetti erogatori quale una delle componenti di front-end del Punto di accesso telematico
[Portale]	L'insieme dei sistemi e delle componenti tecnologiche sviluppate e gestite dal Gestore per la registrazione e gestione dei Soggetti erogatori e l'integrazione tecnologica con il Punto di accesso telematico
[Soggetti erogatori]	I soggetti che rendono fruibili i propri servizi in rete per il tramite del Punto di accesso telematico
[Cittadini]	Un utente del Punto di accesso telematico o un soggetto che necessita di interagire con il Punto di accesso telematico per esercitare un proprio diritto.
[PA]	Pubblica Amministrazione
[WCAG]	Web Content Accessibility Guidelines
[Documentazione API]	La documentazione tecnica per l'integrazione tecnologica dei Servizi tramite API, realizzata e curata dal Gestore
[Interazioni]	I flussi informativi e operativi che avvengono fra l'utente ed il Soggetto Erogatore tramite il Punto di accesso telematico, compreso l'insieme delle azioni a disposizione dell'utente per la fruizione dei servizi esposti dal Soggetto Erogatore
[Messaggi]	Le comunicazioni che un Soggetto erogatore invia tramite il Punto di accesso telematico agli utenti finali
[Moduli]	I singoli elementi e funzionalità del Punto di accesso telematico
[DPIA]	Data Protection Impact Assessment, la valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del GDPR
[Piattaforma PagoPA]	La piattaforma di cui all'art. 5, comma 2 del CAD

Capitolo 3

Principi generali

3.1 Servizio in rete

Nel contesto delle presenti Linee Guida un servizio in rete (di seguito anche solo "**Servizio in rete**") è qualsiasi servizio che uno o più Soggetti erogatori, congiuntamente o disgiuntamente, mettono a disposizione tramite il Punto di accesso telematico per la fruizione da parte degli utenti finali.

Un servizio in rete può consistere in - o comportare - un flusso da un Soggetto erogatore a un utente (es. una PA che deve comunicare un'informazione o un avviso di pagamento a un cittadino) o un flusso da un utente a un Soggetto erogatore (es. un cittadino che richiede a una PA la certificazione di uno stato o che invia un'istanza alla PA).

3.2 Punto di accesso telematico

Il Punto di accesso telematico è l'insieme dei sistemi e delle componenti tecnologiche sviluppate e gestite dal Gestore ai sensi dell'art. 64-bis del CAD.

I Soggetti erogatori DEVONO utilizzare le interfacce esposte dal Punto di accesso telematico per mettere a disposizione agli utenti finali i propri Servizi in rete tramite i canali messi a disposizione dal Gestore.

L'utente finale deve poter accedere al Punto di accesso telematico tramite un'interfaccia disponibile in versione mobile (v. anche 4.2 Obiettivi di semplificazione e principio "once-only", "mobile-first" e di protezione di dati personali) e DEVE poter accedere tramite un'interfaccia versione web.

Il Punto di accesso telematico rappresenta un canale complementare agli altri canali digitali già utilizzati dai Soggetti erogatori. Esso non si sostituisce in alcun modo ai Soggetti erogatori, che rimangono pertanto responsabili dell'erogazione dei propri Servizi in rete e dei relativi trattamenti di dati personali, che restano nella loro disponibilità e responsabilità.

3.3 Gestore

Il gestore del Punto di accesso telematico è la società PagoPA S.p.A., di cui la Presidenza del Consiglio dei Ministri si avvale per la progettazione, lo sviluppo, la gestione e l'implementazione del Punto di accesso telematico, ai sensi dell'articolo 8, commi 2 e 3 del decreto legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla legge 11 febbraio 2019, n. 12.

Il Gestore, nel rispetto delle Linee Guida emanate da AgID, opera secondo le migliori prassi di mercato e tenuto conto dell'evoluzione tecnologica, anche in collaborazione con soggetti terzi di natura pubblica o privata, e PUÒ intraprendere ogni iniziativa e/o misura funzionale al raggiungimento degli obiettivi ad esso affidati dalla Presidenza del Consiglio dei Ministri.

3.4 Soggetti erogatori

I Soggetti erogatori sono i soggetti che rendono fruibili uno o più Servizi in rete tramite il Punto di accesso telematico.

La messa a disposizione di Servizi in rete per il tramite del Punto di accesso telematico è obbligatoria per i soggetti di cui all'articolo 2, comma 2 del CAD, salvo comprovati impedimenti di natura tecnologica e/o organizzativa, attestati dal Gestore ai sensi dell'articolo 64-bis, comma 1-ter del CAD (ad esempio nei casi in cui le caratteristiche del servizio risultano incompatibili con le funzionalità di cui all'Allegato 2 delle presenti Linee guida). È fatta salva la possibilità di rendere fruibili i propri Servizi in rete anche per il tramite di altri canali, che DOVREBBERO essere progettati e sviluppati tenendo in considerazione l'obbligo di garantire l'integrazione e interoperabilità con il Punto di accesso telematico ai sensi dell'articolo 64-bis, comma 1-bis del CAD e nel rispetto dei principi di economicità ed efficienza dell'azione della PA e in conformità con i principi del riuso.

POSSONO rendere fruibili i propri Servizi in rete tramite il Punto di accesso telematico anche soggetti diversi da quelli individuati dall'articolo 2, comma 2 del CAD, previa stipula di apposita convenzione con il Gestore e nel rispetto delle presenti Linee guida.

3.5 Utenti finali dei Servizi in rete

I Servizi in rete DEVONO essere accessibili alle persone fisiche e POSSONO essere accessibili anche a persone fisiche che agiscono per conto di persone giuridiche, se debitamente delegate.

3.6 Documentazione tecnica

Il Gestore DEVE realizzare, mettere a disposizione dei Soggetti erogatori e curare il periodico aggiornamento della documentazione tecnica per l'integrazione tecnologica dei servizi tramite API (di seguito anche "**Documentazione API**") nel rispetto delle linee guida emanate da AgID e, nello specifico, delle [LG INTEROP TEC] e [LG SICUREZZA].

Capitolo 4

Principi per la realizzazione di Servizi in rete e del Punto di accesso telematico

4.1 Accessibilità dei Servizi in rete

Il Gestore DEVE assicurare la semplificazione dell'accesso ai Servizi in rete resi disponibili per il tramite del Punto di accesso telematico nel rispetto dei principi dettati in materia di accessibilità, in conformità alle [LG ACCESSIBILITÀ]:

- *facilità e semplicità d'uso*, da realizzarsi anche attraverso uniformità delle azioni che l'utente finale deve compiere per ottenere l'accesso ai Servizi e alle informazioni;
- *efficienza nell'uso*, per mezzo della separazione tra contenuti, presentazione e modalità di funzionamento delle interfacce, nonché attraverso l'erogazione dei Servizi e delle informazioni mediante differenti canali sensoriali;
- *efficacia nell'uso e rispondenza alle esigenze dell'utente*, anche mediante una erogazione dei Servizi e delle informazioni che prescinda dal dispositivo utilizzato per l'accesso agli stessi;
- *soddisfazione nell'uso*, assicurando l'accesso ai Servizi da parte degli utenti senza ingiustificati disagi o vincoli.

Il Gestore DOVREBBE supportare e guidare i Soggetti erogatori nelle scelte di design necessarie per garantire che le interazioni con gli utenti finali avvengano nel rispetto dei principi di cui sopra.

4.2 Obiettivi di semplificazione, principi in tema di protezione di dati personali, "once-only" e "mobile-first"

Con l'erogazione dei Servizi in rete attraverso il Punto di accesso telematico, il Gestore e i Soggetti erogatori DEVONO perseguire i seguenti obiettivi di semplificazione:

- permettere agli utenti finali di accedere ai Servizi in rete attraverso la propria identità digitale e in modo sicuro, utilizzando SPID o la Carta d'identità elettronica (CIE);

- promuovere Interazioni uniformate e valide per tutti i Soggetti erogatori,conoscibili dall'utente finale e ripetibili ogni volta che sia richiesto lo svolgimento di una stessa serie di operazioni (come ad esempio effettuare pagamenti o richieste), che avvengono seguendo una procedura unica e condivisa indipendentemente dallo specifico Soggetto erogatore coinvolto;
- tali Interazionisono progettate in modo da incorporare flussi e processi semplici, non ridondanti, trasparenti e proporzionati rispetto agli obiettivi dell'azione amministrativa.

L'obiettivo di uniformare le Interazioni per tutti i Soggetti erogatori è favorita dall'applicazione del principio *once-only* o *una tantum* già disciplinato come principio generale dalle [LG DESIGN], secondo cui la PA NON DOVREBBE chiedere ai propri utenti finali informazioni già fornite. Al contrario, ove possibile, la PA DOVREBBE ricorrere alle informazioni già comunicate dagli utenti finali, anche attraverso l'integrazione con le piattaforme previste dal CAD oggetto del successivo paragrafo 5.5 Integrazione del Punto di accesso telematico con le piattaforme previste dal CAD e normative specifiche, nel rispetto delle norme in materia di protezione dei dati e, in particolare, dei principi di necessità e proporzionalità del trattamento di cui al 7.3 Misure di garanzia per le particolari categorie di dati, in modo che sui cittadini e sulle imprese non ricadano oneri aggiuntivi.

In ossequio a tale principio, il Gestore e i Soggetti erogatori DEVONO progettare i Servizi in rete in modo da:

- evitare di richiedere agli utenti finali le stesse informazioni con eccessiva frequenza su più moduli di interazione, e richiedendo una sola volta, all'interno dello stesso flusso, la medesima informazione (*non duplicazione*);
- richiedere esclusivamente le informazioni necessarie alla corretta erogazione dei Servizi in rete (*minimizzazione* e *pertinenza*, rilevanti anche ai fini della protezione dei dati personali);
- garantire un'esperienza dell'utente finale semplice e intuitiva, adeguando a tal fine i rispettivi processi interni quando necessario per il raggiungimento dell'obiettivo.

Nella progettazione dei Servizi in rete sul Punto di accesso telematico il Gestore DOVREBBE valutare, se del caso di concerto con i Soggetti erogatori, l'opportunità di conservare sul dispositivo dell'utente finale le informazioni e le preferenze da questi fornite al fine di poterle riutilizzare nell'erogazione dei Servizi in rete, nel rispetto della normativa in materia di protezione dei dati personali e, con riferimento alle particolari categorie di dati personali, altresì delle misure previste dal 7.3 Misure di garanzia per le particolari categorie di dati.

Il Gestore e i Soggetti erogatori DEVONO assicurare che le fasi di progettazione, sviluppo, test e messa in esercizio dei Servizi in rete sul Punto di accesso telematico avvengano nel rispetto del principio *mobile-first* di cui all'articolo 64-bis, comma 1-ter del CAD. A tal fine, il Gestore guida i Soggetti erogatori:

- mettendo a disposizione, oltre alle [LG DESIGN], l'ulteriore documentazione di dettaglio contenente le regole stilistiche, le librerie, i template e kit di design, conformi alle stesse linee guida che assicurano un'adeguata esperienza utente su dispositivi mobili;
- nella formazione dei Messaggi e delle Interazioni con gli utenti finali tramite il Punto di accesso telematico, con un linguaggio comprensibile e sintetico in grado di essere agevolmente fruibile su dispositivi mobili.

In fase di progettazione e realizzazione del Punto di accesso telematico, il Gestore DEVE assicurare il rispetto dei principi di cui all'articolo 5 del GDPR, garantendo la protezione dei dati personali sin dalla progettazione e per impostazione definita ai sensi dell'articolo 25 del GDPR.

4.3 Rispetto delle minoranze linguistiche e dei principi in materia di accessibilità

Il Punto di accesso telematico DEVE permettere ai Soggetti erogatori di garantire a chiunque il diritto di usare lo stesso in modo accessibile ed efficace in ossequio all'art. 3 del CAD e alle [LG ACCESSIBILITÀ], anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo, fermi restando i diritti delle minoranze linguistiche riconosciute.

Al momento dell'adesione al Punto di accesso telematico e in sede di progressiva implementazione dei Servizi in rete, i Soggetti erogatori nel cui territorio insistono minoranze linguistiche nonché i Soggetti erogatori nazionali - relativamente ai Servizi in rete che interessano anche dette minoranze - trasmettono le informazioni e i contenuti afferenti ai Servizi in rete anche nella diversa lingua minoritariamente insistente nel territorio interessato, sfruttando il layout multilingua del Punto di accesso telematico.

Il Punto di accesso telematico e i Servizi in rete sono resi accessibili e fruibili alle persone con disabilità, in condizioni di uguaglianza rispetto a tutti gli altri utenti. In particolare:

- il Gestore compie ogni ragionevole sforzo per assicurare il rispetto delle norme in materia di accessibilità, con particolare riferimento alle prescrizioni di percepibilità, utilizzabilità, comprensibilità e solidità degli strumenti informatici, permettendo all'utente finale di

svolgere attività (es. attivazione di un servizio, richiesta di assistenza, gestione delle preferenze, ecc.) e di conoscere il dettaglio di ogni Servizio in rete proposto;

- i Soggetti erogatori si impegnano ugualmente al rispetto delle norme di accessibilità per le parti di loro competenza, che riguardano il contenuto dei Servizi in rete, la fruibilità delle informazioni offerte e l'eventuale prosecuzione dell'esperienza all'interno di pagine web o applicazioni fornite dallo stesso Soggetto Erogatore.

I Soggetti erogatori e il Gestore, nell'implementare le soluzioni più efficaci per garantire l'accessibilità, tengono conto dei profili evolutivi del concetto di disabilità, con particolare riferimento alle previsioni della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, che chiarisce che "*la disabilità è il risultato dell'interazione tra persone con minorazioni e barriere attitudinali ed ambientali, che impedisce la loro piena ed efficace partecipazione nella società su una base di parità con gli altri*", e a tal fine collaborano tra loro per raccogliere le necessità degli utenti finali con disabilità al fine di integrare le stesse nei Servizi in rete.

In un'ottica di semplificazione amministrativa, i seguenti adempimenti in materia di accessibilità a carico dei Soggetti erogatori per i Servizi offerti sul Punto di accesso telematico vengono svolti di concerto con il Gestore con le modalità seguenti:

- Il rispetto delle [LG ACCESSIBILITÀ], compresa la **Dichiarazione di accessibilità**, per i Servizi offerti sul Punto di accesso telematico.
- **Meccanismo di feedback**: viene garantito dai Soggetti erogatori, tramite i propri canali istituzionali, e dal Gestore, tramite il sistema di feedback.
- **Obiettivi di accessibilità**: i Soggetti erogatori dichiarano l'obiettivo di offrire i Servizi tramite il Punto di accesso telematico in modalità accessibile entro il 31 marzo dell'anno successivo all'adesione.

I Soggetti erogatori e il Gestore DEVONO garantire, in ogni caso, la riservatezza delle informazioni relative all'utilizzo dei Servizi in rete da parte dei singoli cittadini, anche in conformità alle misure di cui al 7.3 Misure di garanzia per le particolari categorie di dati.

4.4 Open source, sviluppo collaborativo e riuso

Lo sviluppo del Punto di accesso telematico da parte del Gestore privilegia lo sviluppo collaborativo e la standardizzazione tecnologica, anche attraverso l'implementazione dei processi di sviluppo e standard aperti e partecipati di cui alle linee guida applicabili emanate ai sensi dell'articolo 71 del CAD (vedi 2.4 Linee guida di riferimento).

Le componenti software rese pubbliche dal Gestore (es. API e codice sorgente) permettono di proporre integrazioni e miglioramenti ai moduli a partire dal codice condiviso, e allo stesso tempo l'utente finale ha la possibilità, tramite il sistema di feedback, di comunicare al Gestore la sua opinione rispetto alla sua esperienza nell'uso del Punto di accesso telematico. Il Gestore permette lo sviluppo collaborativo da parte dei Soggetti erogatori sui moduli implementati e conserva piena discrezionalità quanto alla revisione e integrazione nel codice sorgente delle modifiche proposte.

La standardizzazione tecnologica, nel rispetto delle linee guida applicabili emanate da AgID (vedi 2.4 Linee guida di riferimento), implica che i moduli devono essere sviluppati in modo da garantire:

- il massimo grado di riuso da parte dei Soggetti erogatori, evitando o riducendo la duplicazione degli sforzi necessari per procedere alle relative implementazioni; e
- il massimo grado di coerenza nell'esperienza degli utenti finali.

Nella realizzazione del Punto di accesso telematico, il Gestore attua quanto disposto dal Capo VI del CAD in merito allo sviluppo, acquisizione e riuso di sistemi informatici nelle PA, applicando le [LG OPEN SOURCE].

Capitolo 5

Punto di accesso telematico

Il Punto di accesso telematico DEVE permettere l'erogazione di Servizi in rete verso gli utenti finali in un'ottica di progressiva multicanalità, nel rispetto del principio *mobile first*.

Il punto di accesso telematico si compone delle seguenti componenti architetturali:

1. un front-end multicanale dedicato alla fruizione dei servizi da parte degli utenti finali,
2. un back office dedicato ai Soggetti erogatori,
3. sistemi back-end che comunicano con i front-end e il back office menzionati e con terze parti di cui integra i servizi.

Il domain model del Punto di accesso telematico è descritto nell'Allegato 4: Domain model del Punto di accesso telematico.

5.1 Front-end per gli utenti finali

Il Punto di accesso telematico si compone di un front-end multicanale, che DEVE includere almeno un'applicazione per dispositivi mobili e tablet ("**App IO**") e una versione web.

Il front-end a sua volta interagisce con il back-end che, tramite interfacce applicative (API) conformi alle [LG INTEROP TEC], abilita la possibilità di usufruire dei Servizi erogati tramite il Punto di accesso telematico.

L'utilizzo del front-end da parte dell'utente finale richiede un'autenticazione forte ai sensi della normativa applicabile, favorendo il massimo livello di sicurezza e il pieno rispetto della privacy.

Successivamente all'autenticazione, l'utente finale PUÒ ricevere e inviare informazioni e, in generale, compiere azioni che vengono gestite dal back-end con eventuali dati provenienti dai sistemi dei Soggetti erogatori o per il tramite dell'eventuale prosecuzione dell'esperienza all'interno di pagine web o applicazioni fornite dallo stesso Soggetto erogatore ove previsto dal Servizio in rete.

L'insieme di funzionalità rese disponibili dai front-end è indicato nell'Allegato 2 e le stesse sono implementate nei limiti delle tecnologie del singolo canale.

5.2 Back-end del Punto di accesso telematico

Il back-end abilita il front-end all'erogazione dell'esperienza di utilizzo personalizzata dell'utente finale identificato in maniera univoca.

Il back-end ricopre inoltre il ruolo di piattaforma abilitante verso i Soggetti erogatori, permettendo l'integrazione con i Moduli del Punto di accesso telematico attraverso API, conformi alle [LG INTEROP TEC] e [LG SICUREZZA], i Soggetti erogatori POSSONO ricevere le richieste degli utenti finali e inviare comunicazioni ai cittadini che utilizzano il Punto di accesso telematico.

La riservatezza dei contenuti dei Messaggi scambiati tra i sistemi dei Soggetti erogatori e i front-end che transitano per la back-end è assicurata dall'applicazione di tecniche di crittografia asimmetrica, ove necessario in relazione alla natura dei dati scambiati dal singolo Servizio in rete. In tale contesto il back-end DOVREBBE assicurare il deployment delle chiavi pubbliche generate per client (il singolo front-end istanziato dall'utente finale) ai sistemi dei Soggetti erogatori. In ogni caso è assicurata l'applicazione di adeguati standard di crittografia a livello di canale.

Il Punto di accesso telematico, nelle transazioni con i sistemi dei Soggetti erogatori, assicura l'attribuzione di un identificativo univoco dei messaggi.

5.3 Back office dedicato ai Soggetti erogatori

Il back office dedicato ai Soggetti erogatori (di seguito "**Portale**") è l'insieme dei sistemi e delle componenti tecnologiche sviluppate e gestite dal Gestore per:

- la registrazione dei Soggetti erogatori al Punto di accesso telematico;
- l'utilizzo da parte dei Soggetti erogatori dei servizi e interfacce messi a disposizione dal Punto di accesso telematico;
- l'integrazione tecnologica dei sistemi dei Soggetti erogatori con il Punto di accesso telematico per il tramite delle API individuate dal Gestore;
- la fornitura di reportistica e analisi del servizio reso dal Gestore per implementare i Servizi in rete per il tramite del Punto di accesso telematico;
- ogni altro servizio che il Gestore rende disponibile ai Soggetti erogatori.

5.4 Repertorio dei Servizi in rete fruibili dal Punto di accesso telematico

Il Gestore DEVE rendere disponibile un repertorio dei Servizi in rete fruibili tramite il Punto di accesso telematico e ne DEVE curare l'aggiornamento.

I Soggetti erogatori DEVONO identificare ciascun Servizio in rete all'interno del Punto di accesso telematico almeno attraverso i seguenti elementi, secondo i formati indicati nelle specifiche per l'identificazione del servizio predisposte dal Gestore:

- identificativo univoco;
- nome: un nome chiaro e riconoscibile per ciascun Servizio in rete, corrispondente a quello impiegato dal Soggetto erogatore negli altri canali a sua disposizione;
- descrizione: descrizione sintetica e chiara del Servizio stesso, con indicazione puntuale delle esigenze collettive che è in grado di assolvere;
- area territoriale: area geografica (locale o nazionale) a cui si riferisce il Servizio in rete del Soggetto erogatore, al fine di permettere all'utente finale di selezionare le aree di proprio interesse;
- identificazione del Soggetto erogatore: esposizione del nome e del logo ufficiale del soggetto che eroga il Servizio in rete;
- link alla documentazione applicabile: ciascun Soggetto erogatore deve esporre, in forma testuale o ipertestuale, nel rispetto delle specifiche tecniche e della documentazione di prodotto trasmessa dal Gestore, la documentazione che regola il rapporto tra il Soggetto erogatore e l'utente finale, compresa la documentazione relativa al trattamento dei dati personali da parte del Soggetto erogatore;
- contatti: i canali e i recapiti di contatto del Soggetto erogatore e degli uffici competenti che l'utente finale può utilizzare per contattare il Soggetto erogatore. Il Soggetto erogatore valuta, di concerto con il Gestore, l'esposizione di un contatto amministrativo e di un contatto tecnico.

5.5 Integrazione del Punto di accesso telematico con le piattaforme previste dal CAD e normative specifiche

In coerenza con il Piano triennale per l'informatica nella Pubblica Amministrazione e, in generale, con il modello strategico di riferimento dell'informatica nella PA, il Punto di accesso telematico DEVE assicurare l'integrazione con le piattaforme tecnologiche che offrono

funzionalità fondamentali, trasversali, abilitanti e riusabili nella digitalizzazione dei processi e dei servizi della PA.

Il Gestore e i soggetti titolari delle singole piattaforme DEVONO assicurare l'interoperabilità del Punto di accesso telematico con le piattaforme di cui all'Allegato 3: Integrazione del Punto di accesso telematico con le piattaforme digitali previste dal CAD e da normative specifiche. A tal fine, i soggetti di cui all'articolo 2, comma 2, i gestori di identità digitali e i prestatori dei servizi fiduciari qualificati DEVONO esporre le API in ottemperanza all'art. 64-bis, comma 1-bis del CAD.

L'integrazione DEVE essere realizzata nel rispetto del modello di interoperabilità delle PA (in breve ModI) e, nello specifico, delle [LG INTEROP TEC], attraverso API individuate dal Gestore in accordo con i soggetti di cui all'articolo 2, comma 2 del CAD, i gestori di identità digitali e i prestatori dei servizi fiduciari che gestiscono le piattaforme di cui all'Allegato 3: Integrazione del Punto di accesso telematico con le piattaforme digitali previste dal CAD e da normative specifiche.

Il Punto di accesso telematico e il soggetto titolare delle singole piattaforme di cui all'Allegato 3: Integrazione del Punto di accesso telematico con le piattaforme digitali previste dal CAD e da normative specifiche DEVONO eseguire la tracciatura delle transazioni realizzate registrando per le singole interazioni almeno:

- la data e l'ora dell'interazione;
- l'identificativo univoco del Soggetto erogatore relativo all'interazione;
- l'esito dell'interazione;
- la risorsa interessata dalla richiesta effettuata dal Punto di accesso telematico alla specifica piattaforma di cui all'Allegato 3: Integrazione del Punto di accesso telematico con le piattaforme digitali previste dal CAD e da normative specifiche.

I soggetti di cui all'articolo 2, comma 2 del CAD, i gestori di identità digitali e i prestatori dei servizi fiduciari qualificati definiscono i livelli di qualità dei Servizi in rete resi disponibili al Punto di accesso telematico in accordo con il Gestore e assicurano il rispetto degli stessi. I livelli di qualità sono definiti a partire dagli indicatori di qualità indicati al successivo paragrafo 6.4 Indicatori di qualità.

5.6 Funzionalità del Punto di accesso telematico

Il Punto di accesso telematico DEVE assicurare le funzionalità previste all'Allegato 2.

Il Gestore PUÒ implementare funzionalità aggiuntive da rendere facoltativamente a disposizione dei Soggetti erogatori anche nelle more dell'aggiornamento dell'Allegato 2. Le funzionalità implementate in maniera aggiuntiva dal Gestore sono semestralmente motivate e comunicate ad AgID che, sentita la Conferenza Unificata istituita dal Decreto Legislativo 28 agosto 1997, n. 281 nel caso di funzionalità che coinvolge le amministrazioni locali, valuta l'aggiornamento del citato Allegato 2.

Capitolo 6

Governance del Punto di accesso telematico

6.1 Adesione dei Soggetti erogatori al Punto di accesso telematico

Il Gestore DEVE gestire l'adesione dei Soggetti erogatori secondo quanto indicato all'Allegato 1: Procedura di adesione dei Soggetti erogatori al Punto di accesso telematico, con modalità idonee a garantire l'onboarding in tempi rapidi e con modalità efficienti per garantire agli utenti finali l'accesso a un numero crescente di Servizi in rete e a tal fine valuta, di concerto con i soggetti coinvolti, l'adesione da parte di PA in forma aggregata ai sensi del 6.1.2 Soggetti aggregatori nonché l'opportunità di avvalersi di partner tecnologici, ai sensi del 6.1.3 Partner tecnologici, anche comuni a più Soggetti erogatori.

Al fine di aderire al Punto di accesso telematico, i Soggetti erogatori DEVONO formalizzare con il Gestore la documentazione contrattuale applicabile, come di seguito descritta.

La documentazione contrattuale standard, eventualmente differenziata per tipologia di Soggetto erogatore, è predisposta dal Gestore e sottoscritta dal Soggetto erogatore, anche per il tramite di eventuali aggregatori o partner tecnologici che agiscono per suo conto sulla base di delega appositamente rilasciata. Tale documentazione contrattuale consta di una lettera di adesione, avente almeno i contenuti di cui all'Allegato 1: Procedura di adesione dei Soggetti erogatori al Punto di accesso telematico e include almeno i seguenti allegati:

- i termini e le condizioni di adesione, di fornitura e di utilizzo del Punto di accesso telematico (T&C);
- l'accordo per il trattamento dei dati personali, contenente la nomina del Gestore quale responsabile del trattamento ai sensi dell'art. 28 del GDPR (DPA);
- l'elenco dei soggetti aggregati (compilato solo ove il Soggetto erogatore sia aggregatore di altre PA ai sensi del 6.1.2 Soggetti aggregatori);
- i termini aggiuntivi applicabili ai Moduli attivati alla data di adesione.

La documentazione contrattuale standard PUÒ essere sostituita o integrata, anche nel tempo, da apposita convenzione predisposta con il Soggetto erogatore e stipulata con lo stesso e/o da ulteriori termini aggiuntivi destinati a regolare i Servizi in rete che richiedano una disciplina specifica e per i quali la documentazione standard non è conferente o sufficiente, nei seguenti casi:

- Servizio in rete i cui termini e condizioni sono definiti da norma primaria o secondaria;
- Servizio in rete che richiede uno sviluppo ad hoc.

6.1.1 Soggetti singoli

Per l'erogazione dei Servizi, i Soggetti erogatori DEVONO:

- identificare le tipologie di Servizi in rete che intendono erogare, in conformità al 6.2 Selezione e sviluppo dei Servizi in rete;
- attivare la procedura di adesione, sottoscrivendo la relativa documentazione contrattuale applicabile, come descritto in premessa al 6.1 Adesione al Punto di accesso telematico dei Soggetti erogatori;
- prendere visione della documentazione correlata al rapporto di adesione al Punto di accesso telematico, con particolare riferimento alle specifiche per l'integrazione tecnologica contenute nella Documentazione API nella versione pubblicata dal Gestore;
- predisporre l'integrazione tra i Sistemi degli enti e il Punto di accesso per il tramite delle API indicate nella Documentazione API previa registrazione al Portale e configurazione dei Servizi in rete;
- eseguire con esito positivo le attività di test ai sensi del 6.2.3 Verifica e test dei Servizi in rete;
- inserire l'anagrafica completa che descrive ciascun Servizio in rete e procedere alla sua attivazione.

I Soggetti erogatori DEVONO rispettare, e garantiscono il rispetto da parte dei propri dipendenti, delegati e/o degli altri soggetti che a qualsiasi titolo agiscono per proprio conto, dei diritti e degli interessi degli utenti finali, sono responsabili del contenuto dei Servizi in rete e utilizzano il Punto di accesso telematico esclusivamente per le finalità istituzionali che gli competono.

Nell'offerta dei propri Servizi in rete, i Soggetti erogatori DEVONO verificare e controllare l'esattezza e l'adeguatezza dei contenuti, nonché la loro conformità alla normativa applicabile.

6.1.2 Soggetti aggregatori

I Soggetti erogatori POSSONO aderire al Punto di accesso telematico in qualità di aggregatori di altri Soggetti erogatori.

L'adesione in forma aggregata DOVREBBE essere privilegiata quando è in grado di garantire la partecipazione, da parte di realtà amministrative di ridotte dimensioni, ai processi di trasformazione digitale, grazie all'accesso a risorse tecniche e organizzative adeguate a mantenere un livello efficiente dei Servizi in rete, nel rispetto dell'autonomia e dell'indipendenza dell'offerta dei servizi locali.

Il rapporto di aggregazione tra Soggetti erogatori, compreso il ruolo rispetto ai trattamenti dei dati personali, è regolato dagli accordi (inclusi gli accordi di cooperazione di cui all'art. 15 della L. 241/1990) e dagli atti amministrativi necessari a conferire al soggetto aggregante i poteri e le attribuzioni necessarie a sottoscrivere il rapporto di adesione anche per conto e a beneficio dei soggetti aggregati, assumendo gli obblighi gravanti sui soggetti aggregati.

I Soggetti erogatori che aderiscono in qualità di aggregatori POSSONO agire in qualità di responsabili del trattamento per conto dei soggetti aggregati ovvero in regime di contitolarità con gli stessi, in base alle rispettive attribuzioni, tenendo conto delle attività di trattamento ad essi demandate.

6.1.3 Partner tecnologici

I Soggetti erogatori e gli aggregatori POSSONO avvalersi di partner tecnologici per lo svolgimento delle attività relative alla gestione dei processi di adesione, di aggregazione e delle attività tecniche necessarie per l'integrazione tecnologica.

In particolare, i Soggetti erogatori POSSONO aderire al Punto di accesso telematico per il tramite di partner tecnologici muniti dei poteri e delle attribuzioni necessarie a sottoscrivere il rapporto di adesione.

I partner tecnologici DEVONO agire unicamente in qualità di responsabili del trattamento per conto dei Soggetti erogatori che se ne avvalgono e in quanto tali sono nominati ai sensi dell'art. 28 GDPR.

6.2 Selezione e sviluppo dei Servizi in rete

Al fine di ampliare l'offerta dei Servizi in rete, il Gestore DEVE mettere a disposizione di tutti i Soggetti erogatori le necessarie API, le cui modalità tecniche sono descritte nella Documentazione API, per l'integrazione dei sistemi dei Soggetti erogatori con il Punto di accesso telematico. I Soggetti erogatori, per la realizzazione dei propri Servizi in rete fruibili per il tramite del Punto di accesso telematico DEVONO attuare le modalità tecniche di integrazione definite nella Documentazione API.

Nel caso di Servizi in rete le cui caratteristiche sono definite da norma primaria o secondaria, il Soggetto erogatore, se del caso di concerto con altri Soggetti erogatori, valuta (o, nel caso di sviluppo definito da una norma, attua) a titolo gratuito o oneroso a seconda dei casi:

- il co-sviluppo con il Gestore;
- l'affidamento dello sviluppo o dell'implementazione al Gestore o, per la parte di back end, ad altro soggetto terzo in collaborazione con il Gestore, fermo restando il rispetto del principio del riuso, ove possibile.

6.2.1 Individuazione del Servizio in rete

6.2.1.1 Catalogo delle tipologie di Servizi in rete

Il Gestore DEVE rendere disponibile un catalogo delle tipologie dei Servizi in rete già disponibili nel Punto di accesso telematico, indicando quando un determinato Servizio in rete è ancora in fase di *beta test*.

I soggetti di cui all'articolo 2, comma 2 del CAD DEVONO prontamente implementare e utilizzare i Servizi in rete già presenti nel catalogo se di interesse per la propria funzione istituzionale. I Servizi in rete in *beta test* sono facoltativi per i soggetti di cui all'articolo 2, comma 2 del CAD fino al loro rilascio in produzione. In caso di rilascio in produzione di un Servizio in rete in *beta test* che coinvolge le amministrazioni locali è necessario acquisire il parere della Conferenza Unificata istituita dal Decreto Legislativo 28 agosto 1997, n. 281 che, in ogni caso, è sentita almeno su base annuale.

6.2.1.2 Definizione di un nuovo Servizio in rete

Qualora sorgesse la necessità di sviluppare un nuovo Servizio in rete, il Soggetto erogatore interessato DEVE farne richiesta al Gestore.

Il Gestore (i) valuta la fattibilità della richiesta, (ii) verifica il possibile interesse per il servizio da parte di altri Soggetti erogatori, (iii) determina i costi e tempi di sviluppo e implementazione, (iv) valuta gli aspetti tecnici, di sicurezza, di conformità alle norme, ivi inclusa la normativa sul trattamento dei dati personali e (v) e comunica le relative risultanze al Soggetto erogatore e PUÒ coinvolgere gli altri soggetti interessati.

I Soggetti erogatori DEVONO affidare lo sviluppo al Gestore, ferma restando la facoltà degli stessi di affidare lo sviluppo e/o la gestione della parte di back end a soggetti terzi, che a tal fine collaborano con il Gestore per la realizzazione del nuovo Servizio in rete.

6.2.2 Realizzazione del Servizio in rete

Il Gestore DEVE definire un piano di lavoro condiviso con il Soggetto erogatore per determinare le reciproche responsabilità al fine di assicurare la messa in esercizio del Servizio in rete. Il suddetto piano di lavoro è redatto nel rispetto delle linee guida emanate da AgID ai sensi dell'articolo 71 del CAD.

Nell'implementazione di un Servizio in rete presente nel catalogo di cui al 6.2.1.1 Catalogo delle tipologie di Servizi in rete, il Gestore definisce un template del piano di lavoro che il Soggetto erogatore DEVE compilare e condividere con il Gestore stesso.

Per l'esecuzione del piano di lavoro il Soggetto erogatore PUÒ avvalersi dei servizi di supporto offerti dal Gestore.

6.2.3 Verifica e test dei Servizi in rete

I Soggetti erogatori DEVONO effettuare i test di integrazione indicati dal piano di test predisposto dal Gestore prima di attivare un Servizio in rete. I test vengono effettuati in ambienti e con utenze dedicate o comunque utilizzando codici fiscali fittizi forniti dal Gestore oppure codici fiscali personali forniti volontariamente dai tester.

6.3 Gestione delle anomalie dei Servizi in rete e assistenza agli utenti finali

Il Gestore e i Soggetti erogatori DEVONO stabilire le responsabilità reciproche.

Il Gestore e i Soggetti erogatori DEVONO rispondere alle anomalie di propria pertinenza, in particolare se dovute a eventi relativi alla sicurezza delle informazioni, in accordo alle procedure documentate e DEVONO assicurare che i meccanismi di segnalazione siano facili, accessibili e disponibili quanto più possibile.

Le anomalie dei Servizi in rete fruiti per il tramite del Punto di accesso telematico DEVONO essere:

- rilevate o segnalate il più velocemente possibile attraverso appropriati canali;
- valutate e classificate (ad esempio, come issue operative, eventualmente legate a vulnerabilità di sistema o di applicazione, o incidenti relativi alla sicurezza delle informazioni) anche al fine di identificare l'impatto e l'estensione di un eventuale incidente.

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza, assicurare che l'uso delle risorse e dei sistemi sia messo a punto in maniera tale da garantire un opportuno presidio, monitoraggio e, quindi, adeguata rilevazione di potenziali eventi anomali.

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza, assicurare che la registrazione degli eventi, delle eccezioni e dei malfunzionamenti sia effettuata, mantenuta e riesaminata periodicamente al meglio delle possibilità, anche attraverso un sistema di monitoraggio automatizzato in grado di generare rapporti consolidati e allarmi su anomalie e sulla sicurezza.

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza e nel rispetto degli artt. 33 e 34 GDPR, definire le procedure di gestione degli eventi anomali per assicurare una risposta rapida, efficace e ordinata in particolare quando questi sono ricondotti a:

- incidenti relativi alla sicurezza delle informazioni e dei dati personali;
- vulnerabilità tecniche sui sistemi o sul software.

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza, prendere in considerazione le seguenti prassi per la gestione degli incidenti:

- pianificazione e preparazione della risposta;
- monitoraggio, per rilevazione e analisi degli eventi/incidenti o dei punti di debolezza relativi alla sicurezza delle informazioni e dei dati personali;
- valutazione e presa di decisione;

- regole per escalation, ripristino controllato e comunicazione verso stakeholder interni ed esterni.

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza, registrare i risultati delle valutazioni e delle decisioni prese, la conoscenza acquisita dall'analisi e dalla soluzione delle anomalie al fine di utilizzarle per ridurre l'impatto degli incidenti futuri.

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza, intraprendere azioni appropriate e tempestive per rispondere all'identificazione di potenziali vulnerabilità tecniche, attraverso un processo per la loro gestione efficace (monitoraggio, valutazione del rischio, azioni di riduzione). Le informazioni sulle vulnerabilità tecniche DEVONO essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità DEVE essere valutata e appropriate misure DEVONO essere intraprese per affrontare i rischi relativi:

- definendo una scala temporale per reagire alle notifiche di vulnerabilità tecniche potenzialmente pertinenti;
- identificando una potenziale vulnerabilità tecnica e determinandone i rischi relativi e le azioni da intraprendere tra cui l'applicazione delle patch ai sistemi vulnerabili o l'adozione di altri controlli;
- portando a termine le azioni intraprese coerentemente con:
    - loro urgenza;
    - controlli collegati alla gestione dei cambiamenti;
    - procedure di risposta agli incidenti relativi alla sicurezza delle informazioni e dei dati personali (per comunicare dati sulle vulnerabilità alle funzioni adibite alla risposta agli incidenti e per fornire procedure tecniche da eseguire in caso di incidente);
    - test e valutazione delle soluzioni individuate, per assicurare che siano efficaci e non comportino effetti collaterali intollerabili, o valutazione dei rischi e individuazione di appropriate azioni di individuazione e correzione in caso non esista (ancora) una contromisura adatta.

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza, mantenere un log di audit di tutte le procedure intraprese.

-

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza, mettere a disposizione degli utenti finali efficaci canali per riportare e segnalare le anomalie riscontrate e DEVONO definire tempi di risposta certi alle segnalazione ricevute.

I Soggetti erogatori, tramite i propri canali istituzionali, e il Gestore, tramite apposito sistema di feedback, DEVONO rispondere prontamente alle richieste degli utenti finali nel rispetto degli indicatori di qualità di cui 6.4.4 Indicatori dei servizi di supporto.

I Soggetti erogatori e il Gestore, per le parti di rispettiva competenza, DEVONO altresì svolgere attività di ricerca e coinvolgimento degli utenti finali per monitorare il livello di qualità e individuare i miglioramenti necessari rispetto ai Servizi offerti tramite il Punto di accesso telematico:

- in fase di analisi e progettazione, consultando i cittadini nell'identificazione e nella definizione dei Servizi e delle funzionalità da veicolare attraverso il Punto di accesso telematico;
- in fase di sviluppo e test, coinvolgendo i cittadini, con particolare riferimento ad alcune categorie, nella validazione dei modelli e dei contenuti proposti;
- in fase di produzione, raccogliendo il feedback dei cittadini sull'utilizzo dei Servizi e sui requisiti per successive implementazioni.

6.4 Indicatori di qualità

Il rapporto tra Gestore e Soggetti erogatori in merito ai Servizi in rete è regolato dai livelli di qualità attesi nell'erogazione degli stessi, nello specifico sono oggetto di interesse:

- i Servizi in rete individuati in accordo dal Soggetto erogatore e Gestore;
- il piano di lavoro, condiviso tra Gestore e Soggetto erogatore, per la realizzazione dei Servizi in rete;
- deliverable realizzati dal Gestore, dal Soggetto erogatore o da terze parti per conto degli stessi, in attuazione del piano di lavoro per la realizzazione dei Servizi in rete;
- API realizzate dal Soggetto erogatore per assicurare l'integrazione con il Punto di accesso telematico, funzionali alla messa in esercizio dei Servizi in rete;
- servizi di supporto assicurati dal Gestore per la realizzazione e manutenzione dei Servizi in rete;
- servizi di supporto agli utenti da parte del Gestore e del Soggetto erogatore.

In quanto segue si riportano un primo insieme di indicatori di qualità utilizzati dal Gestore e i Soggetti erogatori per definire gli accordi sui livelli di qualità dei servizi che il Gestore garantisce ai Soggetti erogatori e che i Soggetti erogatori garantiscono agli utenti finali.

Gli stessi indicatori di qualità sono utilizzati dal Gestore e dai Soggetti di cui all'articolo 2, comma 2, dai fornitori di identità digitali e dai prestatori dei servizi fiduciari qualificati per concordare i livelli di qualità assicurati dai servizi resi disponibili, da questi ultimi, al Punto di accesso telematico in ottemperanza al comma 1-bis dell'articolo 64-bis del CAD.

6.4.1 Indicatori sulla qualità dello sviluppo

6.4.1.1 Difettosità in avvio

Il presente indicatore rileva la difettosità residua funzionale e non funzionale all'avvio di un servizio/API. Nello specifico:

- sono raccolti l'aderenza ai requisiti di accessibilità, usabilità, sicurezza e prestazioni per permettere la piena fruizione delle funzionalità dei Servizi in rete da parte degli utenti finali;
- sono raccolti l'aderenza ai requisiti di sicurezza e prestazioni per permettere la piena fruizione delle funzionalità delle API realizzate.

L'indicatore è determinato come rapporto tra il numero di requisiti funzionali e non funzionali del servizio/API non soddisfatti in fase di collaudo e il numero di requisiti funzionali e non funzionali dello stesso servizio/API individuati dai requirements dello stesso.

6.4.1.2 Difettosità in avvio in esercizio

Il presente indicatore rileva la difettosità residua funzionale e non funzionale nell'esercizio di un servizio. Nello specifico:

- sono raccolti l'aderenza ai requisiti di accessibilità, usabilità, sicurezza e prestazioni per permettere la piena fruizione delle funzionalità dei Servizi in rete da parte degli utenti finali;
- sono raccolti l'aderenza ai requisiti di sicurezza e prestazioni per permettere la piena fruizione delle funzionalità delle API realizzate.

L'indicatore è determinato come rapporto tra il numero di requisiti funzionali e non funzionali del servizio/API non soddisfatti determinati in esercizio e il numero di requisiti funzionali e non funzionali dello stesso servizio/API individuati dai requirements dello stesso.

6.4.2 Indicatori del piano di lavoro

6.4.2.1 Rispetto del piano di lavoro

L'indicatore verifica il rispetto della pianificazione del piano di lavoro misurando il rispetto della scadenza temporale di ciascuna milestone (determinazione dello scostamento tra data prevista e data effettiva), quali ad esempio:

- la date di consegna degli artefatti;
- per i cicli agili, ogni data pianificata nello Sprint Planning;
- la data pianificata di "pronti al collaudo";
- la data pianificata di termine collaudo con esito positivo;
- la data pianificata di avvio in esercizio.

Eventuali ripianificazione del piano di lavoro determinato da ritardi causati da problematiche relative alle API realizzate dal Soggetto erogatore non sono in alcun modo imputabili al Gestore.

6.4.2.2 Giorni di sospensione del collaudo

La sospensione del collaudo è indice di una grave carenza qualitativa e incompletezza delle attività realizzative. La sospensione può attivarsi automaticamente alla presenza di malfunzionamenti bloccanti in collaudo o su decisione del Soggetto erogatore qualora si verifichino situazioni "anomale" che, a giudizio dello stesso, sia per numerosità sia per gravità, sia per non rispetto dei tempi massimi previsti per la risoluzione delle difformità, non consentano lo svolgimento o la prosecuzione delle attività di collaudo.

L'indicatore è determinato dal tempo trascorso tra la sospensione del collaudo e il suo riavvio.

Ogni impedimento determinato da problematiche relative alle API realizzata dal Soggetto erogatore non sono in alcun modo imputabili al Gestore.

6.4.3 Indicatori dei servizi/API realizzati

6.4.3.1 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. 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 in accordo tra il Gestore e il Soggetto erogatore 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 dal Gestore.

6.4.3.2 Numero di richieste per unità di tempo

Il numero di richieste soddisfatte da un servizio/API è indice della capacità di carico gestibile dallo stesso.

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 in accordo tra il Gestore e il Soggetto erogatore 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 dal Gestore.

6.4.3.3 Numero di richieste con risposta non di errore per unità di tempo

Il numero di richieste con risposta non di errore di un servizio/API è indice dell'efficacia dello stesso.

Il presente indicatore è determinato del numero di request non di errore nell'unità di tempo. L'unità di tempo per la determinazione dell'indicatore è individuata in accordo tra il Gestore e il Soggetto erogatore per singolo servizio/API, ad esempio numero di request non di errore in 10 minuti. Si evidenzia che tale indicatore è direttamente proporzionale all'efficacia del servizio/API.

La fonte per la determinazione del numero di request non di errore è rappresentato dai log file tenuti dal Gestore.

6.4.4 Indicatori dei servizi di supporto

6.4.4.1 Tempestività di ripristino dell'operatività

Il presente indicatore si applica a non conformità funzionali e non funzionali rilevate ed è calcolato come la differenza in ore tra il momento dell'avvio del processo di risoluzione del malfunzionamento e il termine della risoluzione dello stesso.

6.4.4.2 Tempestività di risposta a segnalazioni di anomalie

Il presente indicatore si applica a non conformità funzionali e non funzionali evidenziate dal Soggetto erogatore e/o dagli utenti finali dei Servizi in rete. L'indicatore è calcolato come la differenza in ore tra il momento della segnalazione e la presa in carico della stessa da parte del Gestore.

Il presente indicatore si applica anche a non conformità funzionali e non funzionali evidenziate dal Gestore e/o dagli utenti finali dei Servizi in rete. L'indicatore è calcolato come la differenza in ore tra il momento della segnalazione e la presa in carico della stessa da parte del Soggetto erogatore.

Capitolo 7

Disposizioni in materia di sicurezza e protezione dei dati personali

7.1 Trattamenti e ruoli dei soggetti coinvolti

Il Gestore agisce come titolare del trattamento per le seguenti finalità, determinando le modalità e i mezzi attraverso cui i relativi trattamenti DEVONO essere effettuati e definendo altresì le scelte implementative all'uopo necessarie:

- attività necessarie alla progettazione, allo sviluppo, alla gestione e all'implementazione del Punto di accesso telematico, ivi incluse le attività volte a permettere l'interoperabilità del Punto di accesso telematico con le piattaforme abilitanti di cui all'Allegato 3: Integrazione del Punto di accesso telematico con le piattaforme digitali previste dal CAD e da normative specifiche nonché le relative attività di assistenza, debugging e diagnostica, monitoraggio del funzionamento, utilizzo del Punto di accesso telematico e miglioramento ed evoluzione dello stesso (ricerca e sviluppo), nel rispetto di quanto stabilito al 7.5.4 Anonimizzazione dei dati personali;
- attività effettuate con riguardo alle funzionalità e/o servizi direttamente resi dal Gestore al Cittadino su sua richiesta, ivi incluse quelle che permettano al Cittadino di gestire in modo agevole e dinamico la propria relazione con i Soggetti erogatori per i servizi erogati per il tramite del Punto di accesso telematico;
- altre attività che gli sono attribuite ai sensi di legge per l'esecuzione di compiti di interesse pubblico.

I Soggetti erogatori agiscono come titolari del trattamento (o, in alcuni casi, responsabili del trattamento di altre PA) con riguardo ai singoli trattamenti svolti tramite il Punto di accesso telematico secondo la base giuridica corrispondente allo specifico Servizio in rete offerto.

Qualora un Soggetto erogatore agisca come responsabile di un'altra PA, mettendo a disposizione i Servizi in rete per conto di quest'ultima, lo stesso DEVE aver stipulato un accordo ai sensi dell'art. 28 del GDPR.

Fuori dalle attività di trattamento effettuate in qualità di titolare, con particolare riferimento ai dati trattati per la finalità di erogazione dei Servizi in rete, il Gestore agisce in qualità di responsabile del trattamento (o, se del caso, sub-responsabile del trattamento), sulla base di un accordo ai sensi dell'art. 28 del GDPR. A sua volta il Gestore PUÒ avvalersi di terzi sub-responsabili nel rispetto di quanto previsto dall'art. 28 del GDPR.

Le comunicazioni di dati personali, diversi dai dati di cui agli artt. 9 e 10 del GDPR, da un Soggetto erogatore a un'altra PA ovvero al o dal Gestore, sono ammesse se necessarie ai fini dell'erogazione di Servizi in rete richiesti dai Cittadini al Gestore o al Soggetto erogatore, nel rispetto dei principi di cui all'art. 5 del GDPR, con particolare riferimento ai principi di liceità, trasparenza, limitazione della finalità e minimizzazione dei dati, nonché nei limiti di quanto previsto dall'art. 2-ter del Codice Privacy.

7.2 Misure di sicurezza per l'erogazione di Servizi in rete

Il Gestore e i Soggetti erogatori DEVONO implementare almeno le misure indicate nell'Allegato 5, ferma restando - ai sensi dell'art. 32 del GDPR e nel rispetto del principio di responsabilizzazione - la necessaria predisposizione di ogni misura tecnica e organizzativa adeguata a garantire un livello di sicurezza adeguato al rischio.

In ottica di data protection by design e by default e con riferimento alla natura, al contesto e ai trattamenti connessi a uno specifico Servizio in rete, il Gestore e il Soggetto erogatore POSSONO concordare misure organizzative e tecniche aggiuntive rispetto a quanto previsto nell'accordo stipulato ai sensi dell'art. 28 del GDPR. Qualora un Soggetto erogatore offra diverse tipologie di Servizi in rete, le misure di sicurezza POSSONO essere diversificate anche rispetto ai singoli Servizi in rete. In tali casi, le misure concordate integreranno l'accordo di cui all'art. 28 del GDPR e saranno considerate come istruzioni rese al responsabile del trattamento.

7.3 Misure di garanzia per particolari categorie di dati

Ai sensi degli artt. 9, paragrafo 2 e 10 del GDPR nonché degli artt. 2-sexies, 2-septies e 2-octies del Codice Privacy, il Gestore, al fine di porre in essere le attività di progettazione, sviluppo, gestione e implementazione del Punto di accesso telematico nonché altre attribuite dalla legge o delegate dagli utenti, PUÒ trattare anche particolari categorie di dati personali mediante misure

appropriate e specifiche per tutelare i diritti fondamentali e le libertà dell'interessato. Tali particolari categorie di dati sono trattate sulla base dell'interesse pubblico il cui perseguimento è affidato al Gestore dalla legge e, in particolare, dai commi 2 e 3 dell'art. 8 del D. Lgs. 135/2018 e dall'art. 64-bis del CAD.

In particolare, POSSONO essere trattati tramite il Punto di accesso telematico particolari categorie di dati personali per attività di raccolta, elaborazione e comunicazione ad altre PA, nel rispetto dei diritti degli interessati. Eventuali Messaggi contenenti tali categorie particolari di dati personali DEVONO essere richiesti dall'utente e il trattamento DEVE svolgersi unicamente laddove sia indispensabile per l'erogazione dei Servizi in rete forniti dai Soggetti erogatori ovvero di servizi altrimenti richiesti dagli utenti al Gestore.

In ogni caso, laddove i Soggetti erogatori trattino categorie particolari di dati personali, al fine di offrire i Servizi in rete tramite il Punto di accesso telematico, questi DEVONO:

a. individuare le particolari categorie di dati indispensabili all'erogazione del Servizio in rete tramite il Punto di accesso telematico secondo quanto previsto dal precedente 7.4.1 Minimizzazione;
b. darne informazione al Gestore;
c. non comunicare tali particolari categorie di dati nell'oggetto del messaggio e assicurarne la minimizzazione all'interno del corpo del messaggio stesso;
d. utilizzare gli strumenti messi a disposizione dal Gestore per classificare un contenuto come contenente categorie particolari di dati, al fine di differenziare le modalità di trattamento dei predetti dati all'interno del Punto di accesso telematico, in conformità ai principi di privacy by default e by design;
e. laddove presenti, utilizzare gli altri strumenti messi a disposizione dal Gestore per contrassegnare i messaggi o i Servizi dal contenuto sensibile.

7.4 Necessità e proporzionalità del trattamento

7.4.1 Minimizzazione

I Soggetti erogatori, nel mettere a disposizione i propri Servizi in rete, DEVONO ridurre il trattamento ai soli dati strettamente necessari per la fornitura dei Servizi stessi.

A tal fine, i Soggetti erogatori, prima di mettere in produzione i propri Servizi in rete, DEVONO:

a. fare una ricognizione dei dati personali che vengono trattati per ciascun Servizio in rete;
b. individuare le relative categorie, la finalità per cui sono trattati e la base giuridica;
c. assicurarsi che l'informativa sul trattamento dei dati personali, che verrà resa agli interessati, rispecchi l'effettivo trattamento che verrà effettuato tramite il Punto di accesso telematico, come specificato al 7.4.4 Trasparenza e rispetto dell'esercizio dei diritti degli utenti finali.

In particolare, i Soggetti erogatori DEVONO:

a. essere in grado di comprovare, nel rispetto del principio di responsabilizzazione, che i dati personali siano sufficienti, pertinenti, necessari e non eccessivi rispetto alla finalità perseguita;
b. essere in grado di comprovare, nel rispetto del principio di responsabilizzazione, che i dati personali non rivelino (direttamente o indirettamente) l'origine razziale o etnica, le opinioni politiche, filosofiche o religiose, l'appartenenza sindacale, le informazioni sulla salute o sulla vita sessuale di un individuo, tranne che nei casi in cui sia strettamente indispensabile per l'erogazione del Servizio;
c. essere in grado di comprovare che i dati personali non si riferiscono a reati, sentenze penali o misure di sicurezza, salvo che ciò sia espressamente previsto da una norma di legge, ovvero, dove previsto dalla legge, di regolamento;
d. evitare il trattamento di dati personali eccessivi o ulteriori rispetto alla finalità dei Servizi in rete;
e. istruire i soggetti designati al trattamento al fine di limitare il trattamento di dati personali nel contesto dell'invio di messaggi e comunicazioni ai cittadini secondo un principio di stretta necessità;
f. limitare allo stretto necessario la trasmissione di documenti elettronici contenenti dati personali;
g. adempiere gli obblighi informativi previsti dal GDPR, come specificato al 7.4.4 Trasparenza e rispetto dell'esercizio dei diritti degli utenti finali.

7.4.2 Limitazione dei tempi di conservazione

Il Gestore e i Soggetti erogatori, al fine di garantire il rispetto del principio di limitazione della conservazione e per ridurre l'impatto dei rischi, DEVONO assicurarsi che i dati personali

non vengano mantenuti per più tempo di quanto necessario. In particolare, il Gestore e i Soggetti erogatori DEVONO:

a. definire periodi di conservazione dei dati personali limitati nel tempo e appropriati rispetto alle finalità del trattamento;
b. implementare misure tecniche e/o organizzative che consentano di rilevare la scadenza del periodo di conservazione;
c. 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 alle libertà civili e alla privacy dei soggetti interessati;
d. eliminare i dati personali quando il periodo di conservazione definito nella relativa procedura scade.

Al fine di assistere i Soggetti erogatori nell'assicurare il rispetto di tali disposizioni ed evitare i rischi connessi a duplicazioni di dati personali, il Gestore conserva i dati trattati per conto dei Soggetti erogatori sui propri sistemi per un periodo di tempo limitato, individuato nell'accordo ex art. 28 del GDPR, che sia ragionevole e che consenta un'efficiente gestione tecnologica del Punto di accesso telematico.

7.4.3 Misure di responsabilizzazione - cd. principio di "accountability"

Il Gestore DEVE predisporre una valutazione d'impatto sulla protezione dei dati personali e consultare il Garante per la protezione dei dati personali, ai sensi degli artt. 35-36 del GDPR.

Tale DPIA è messa a disposizione dei Soggetti erogatori e contiene un'appendice sui trattamenti che gli stessi possono facoltativamente utilizzare come ausilio per completare la propria valutazione d'impatto con riguardo ai trattamenti rispetto ai quali sono titolari ulteriori rispetto a quelli coperti dalla DPIA del Gestore e non oggetto di autonoma DPIA.

I Soggetti erogatori consultano il Garante per la protezione dei dati personali ai sensi degli artt. 35 e 36 del GDPR unicamente qualora la valutazione d'impatto sui propri trattamenti, ulteriori rispetto a quelli oggetto della DPIA del Gestore e distinti dal mero utilizzo del Punto di accesso telematico, individui un rischio elevato in assenza di misure adottate dal titolare del trattamento per

attenuare tale rischio, nonostante le misure già contenute nella DPIA del Gestore e nelle presenti Linee guida e non coperto da queste ultime.

I Soggetti erogatori DEVONO, inoltre, aggiornare il proprio registro delle attività di trattamento, ai sensi dell'art. 30 del GDPR, indicando le attività svolte tramite il Punto di accesso telematico e i relativi dati trattati.

7.4.4 Trasparenza e rispetto dell'esercizio dei diritti degli utenti finali

La trasparenza è una condizione di garanzia delle libertà individuali nonché dei diritti civili, politici e sociali.

Pertanto il Gestore, per quanto concerne i trattamenti di propria titolarità, e i Soggetti erogatori, per quanto concerne i propri Servizi in rete, DEVONO fornire, mediante il Punto di accesso telematico, un'informativa completa dei trattamenti dei dati personali, nel rispetto degli artt. 12-13-14 del GDPR.

Se i Soggetti erogatori agiscono in qualità di responsabili del trattamento per conto di un'altra PA, si assicurano che agli interessati sia fornita un'adeguata informativa comprensiva di tutti i requisiti di cui agli art. 13 e 14 GDPR.

I Soggetti erogatori DEVONO adottare misure organizzative adeguate a garantire l'esercizio dei diritti degli interessati rispetto ai dati trattati per l'erogazione dei Servizi in rete. A tal fine, i Soggetti erogatori DEVONO fornire un recapito che il Gestore PUÒ contattare laddove riceva una richiesta di esercizio dei diritti per i trattamenti di cui è responsabile e che rimane a disposizione degli utenti nell'utilizzo del Punto di accesso telematico.

I Soggetti erogatori gestiscono le richieste di esercizio di diritti di cui agli artt. 15 e seguenti del GDPR in autonomia, valutandone i presupposti e chiedendo supporto al Gestore laddove necessario e senza che ciò possa comportare sforzi irragionevoli. Il Gestore PUÒ offrire, in un'ottica di privacy by design, funzionalità atte a garantire un più facile esercizio dei diritti degli interessati, qualora ciò non comporti uno sforzo irragionevole.

7.4.5 Trasferimenti dei dati personali e responsabili del trattamento.

Ai fini della fornitura del Punto di accesso telematico, il Gestore PUÒ fare ricorso a soggetti terzi, opportunamente nominati propri responsabili del trattamento ai sensi dell'art. 28 del GDPR, e se ne avvale nel rispetto del principio di responsabilizzazione.

Il Gestore, per le attività nelle quali agisce in qualità di responsabile del trattamento, DEVE mettere a disposizione dei Soggetti erogatori la lista aggiornata dei propri responsabili del trattamento.

Il Gestore DEVE privilegiare, a parità di garanzie, fornitori situati sul territorio nazionale e dell'Unione Europea. In ogni caso, laddove possibile, il Gestore DEVE istruire i responsabili del trattamento sulla necessità di conservare i dati all'interno dell'Unione Europea.

Laddove non sia possibile trovare un responsabile del trattamento nell'Unione Europea che offra garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate alla sicurezza dei trattamenti e alla tutela dell'interessato, il Gestore PUÒ ricorrere a responsabili situati in Paesi terzi, 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'art. 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, e ove possibile richiedere l'implementazione di misure supplementari al fine di impedire l'identificazione dell'interessato da parte del responsabile e/o da autorità governative straniere, anche in ossequio a quanto previsto al 7.5.3 Cifratura dei dati personali.

Il Gestore DEVE, in ogni caso, rispettare le misure previste dal Capo V del GDPR. Laddove necessario, il Gestore pone in essere misure contrattuali necessarie (ad esempio, clausole contrattuali tipo) anche per conto dei Soggetti erogatori.

7.5 Sicurezza del trattamento

7.5.1 Principi

In conformità all'art. 32 e al Considerando 83 del GDPR, il Gestore e i Soggetti erogatori, in qualità di titolari del trattamento e/o responsabili del trattamento, sono tenuti ad adottare tutte le misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio; tali misure comprendono, tra le altre, se del caso:

a. la pseudonimizzazione e la cifratura 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. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

I principi in materia di sicurezza del trattamento si esplicitano nelle seguenti "*best practices*" per il trattamento dei dati personali, che si aggiungono alle misure organizzative implementate per garantire il rispetto dei principi in materia di trattamento di dati personali di cui ai precedenti paragrafi.

7.5.2 Partizionamento dei dati personali

Il Gestore e i Soggetti erogatori DEVONO ridurre la possibilità che i dati personali raccolti e trattati per determinate finalità possano essere correlati con dati raccolti e trattati per finalità diverse e DEVONO applicare, per quanto possibile, misure tecniche e organizzative di segregazione dei dati. Il Gestore e i Soggetti in particolare DEVONO:

a. identificare i dati personali utili alle finalità perseguite e utilizzare il set minimo di dati necessari, anche nell'ambito del singolo processo, in virtù del principio di minimizzazione;
b. separare i dati necessari per ogni processo in modo logico;
c. essere in grado di comprovare che i dati personali siano partizionati in modo efficace.

7.5.3 Cifratura dei dati personali

Il Gestore e i Soggetti erogatori DEVONO 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.

7.5.4 Aggregazione dei dati personali

Nel perseguimento delle finalità di cui al 7.1 Trattamenti e ruoli dei soggetti coinvolti, ogni qualvolta possibile, il Gestore , DEVE utilizzare dati aggregati o pseudonimizzati, in conformità al principio di minimizzazione di cui all'art. 5 del GDPR. In particolare, il Gestore DEVE utilizzare dati aggregati in modo che non se ne possa trarre alcun riferimento relativamente a persone identificate o identificabili, in conformità al principio di minimizzazione. In particolare il Gestore PUO' trattare dati aggregati:

:a:

- per finalità di monitoraggio del funzionamento e utilizzo del Punto di accesso telematico e di miglioramento ed evoluzione dello stesso (ricerca e sviluppo);
- per una generale finalità di trasparenza rispetto ai compiti affidati al Gestore e relativi alla progettazione, allo sviluppo, alla gestione e all'implementazione del Punto di accesso telematico e agli altri compiti affidati al Gestore in forza di legge o in applicazione di norme di legge, inclusa l'informazione ai cittadini e al pubblico nel suo complesso, nonché l'attività di relazione che, nel rispetto degli obblighi ad esso facenti capo, il Gestore è tenuto a svolgere periodicamente verso i Soggetti erogatori e le istituzioni.

7.5.5 Dati di log

Al fine di garantire la sicurezza del trattamento e svolgere attività di sviluppo e gestione, nonché di rispondere a eventuali richieste dei Soggetti erogatori relativamente alle attività svolte tramite il Punto di accesso telematico, il Gestore DEVE raccogliere dati di log relativamente alle richieste inviate da ciascun Soggetto erogatore e li DEVE conservare per un tempo predeterminato e ragionevole alla luce delle finalità perseguite e periodicamente individuate nella valutazione di impatto, nel rispetto del principio di responsabilizzazione..

In particolare, tali log DEVONO contenere almeno le seguenti informazioni:

- la data e l'ora della richiesta;
- l'identificativo univoco del Soggetto erogatore;
- l'esito della richiesta;

- la risorsa logica interessata dalla richiesta;
- ove necessario, l'identificativo univoco del soggetto interessato.

Le presenti Linee guida non pregiudicano altre normative, linee guida o regolamenti che comportano obblighi di conservazione di dati di log diversi da quelli oggetto del presente paragrafo.

7.5.6 Accesso dei soggetti autorizzati

Il Gestore e i Soggetti erogatori DEVONO:

- essere consapevoli delle procedure per segnalare gli eventi anomali e del punto di contatto al quale gli eventi sono segnalati;
- monitorare l'uso delle proprie risorse e sistemi per una adeguata rilevazione di potenziali eventi anomali, ulteriore rispetto a quanto effettuato dal Gestore, registrando e riesaminando periodicamente eventi, eccezioni e malfunzionamenti;
- segnalare il più velocemente possibile ogni evento anomalo, in particolare se ritenuto relativo alla sicurezza delle informazioni e dei dati personali;
- collaborare con il Gestore nella valutazione e classificazione degli eventi;
- comunicare in maniera tempestiva le informazioni sulle potenziali vulnerabilità tecniche che dovessero rilevare;
- correggere eventuali anomalie, rispettando (sulla base delle responsabilità individuate e delle istruzioni fornite) le indicazioni del Gestore per la risoluzione di incidenti e/o vulnerabilità;
- autorizzare e istruire adeguatamente il proprio personale e i collaboratori ai sensi dell'art. 29 del GDPR, designandoli ai sensi dell'art. 2-quaterdecies del Codice privacy anche con riferimento ai punti sopra indicati.

I Soggetti erogatori utilizzano il Portale per il tramite degli utenti da essi indicati attraverso le funzionalità rese disponibili dal Gestore. Il Gestore DEVE assicurare con cadenza periodica:

- l'individuazione dei Soggetti Erogatori che non hanno dato seguito alla verifica periodica delle proprie utenze;
- l'individuazione dei comportamenti anomali (ad esempio utilizzo fuori dai normali orari di lavoro, numero di accessi ripetuti in un breve lasso di tempo, ecc.).

7.5.7 Continuità operativa e disaster recovery

Il Gestore e i Soggetti erogatori DEVONO, per le parti di propria competenza, predisporre, considerate le [LG RECOVERY], adeguati piani di continuità operativa per il ripristino delle condizioni anomale, includendo tutti i necessari accorgimenti per il backup e per il ripristino di dati e del software.

Allegato 1: Procedura di adesione dei Soggetti erogatori al Punto di accesso telematico

Il presente allegato descrive la procedura di adesione dei Soggetti erogatori al Punto di accesso telematico tramite il Portale.

1. Contenuto dell'accordo di adesione

L'accordo di adesione è predisposto dal Gestore in modo standardizzato, applicabile a tutti i Soggetti erogatori e non modificabile, salvo i casi di accordi di cui al penultimo e all'ultimo periodo del 6.1 Adesione al Punto di accesso telematico dei Soggetti erogatori e contiene almeno gli elementi relativi all'identificazione del Soggetto erogatore, del soggetto firmatario e dei soggetti delegati ad operare per conto del Soggetto erogatore nell'ambito del Punto di accesso telematico, nonché la durata dell'accordo di adesione e il suo meccanismo di rinnovo e, altresì, gli obblighi e garanzie delle parti rispetto alla normativa sul trattamento di dati personali. Nello stesso accordo di adesione sono individuati ruoli e responsabilità del Gestore e dei Soggetti erogatori relativamente all'eventuale applicazione della federated identity, secondo le regole tecniche di cui al paragrafo 1 dell'Allegato 2.

2. Perfezionamento dell'accordo di adesione e comunicazione dei soggetti delegati

I Soggetti erogatori POSSONO aderire autonomamente o avvalersi di delegati, preventivamente comunicati al Gestore, eventualmente scelti tra i propri partner tecnologici (vedi 6.1.3 Partner tecnologici).

Il rapporto tra il Soggetto erogatore e i propri delegati DEVE essere regolato da appositi accordi, in grado di conferire a questi ultimi i poteri necessari e di disciplinarne gli obblighi.

Il Soggetto erogatore DEVE informare tempestivamente il Gestore in caso di modifica e/o cessazione dei poteri di delega.

In particolare, il perfezionamento dell'accordo di adesione e la comunicazione al Gestore dei soggetti delegati dal Soggetto erogatore a operare nel Punto di accesso telematico per suo conto

avvengono secondo il seguente processo, salvo i casi di accordi di cui al penultimo e all'ultimo periodo del 6.1 Adesione al Punto di accesso telematico dei Soggetti erogatori.

Il processo per il perfezionamento dell'accordo di adesione consta delle seguenti azioni:

1. una persona fisica, previa autenticazione forte, entra nel Portale e dichiara di appartenere a un determinato Ente.
2. il Portale invia una comunicazione al domicilio digitale dell'Ente con:
    a. la contrattualistica standard di cui al 6.1 Adesione al Punto di accesso telematico dei Soggetti erogatori
    b. un link per perfezionare il predetto accordo;
    c. il nominativo e il codice fiscale della persona di cui al punto 1 che ha avviato il processo.
3. L'Ente firma digitalmente l'accordo di adesione.
4. L'Ente accede al link ricevuto via domicilio digitale per:
    a. caricare l'accordo di adesione firmato digitalmente;
    b. nominare almeno un rappresentante, indicandone il codice fiscale e delegando lo stesso ad agire all'interno del Portale per proprio conto;
    c. confermare l'iscrizione dell'Ente al Portale.
5. Il Portale verifica le informazioni inviate e perfeziona o meno l'iscrizione.
6. Se l'iscrizione è perfezionata, il/i rappresentante/i nominato/i è/sono abilitato/i all'accesso al Portale, tramite autenticazione forte, per conto del Soggetto erogatore.

3. Gestione dei delegati del Soggetto erogatore nel Portale

Durante la fase di perfezionamento dell'accordo di adesione, i Soggetti erogatori DEVONO indicare uno o più referenti amministrativi, i quali a loro volta, tramite il Portale cui si accede secondo le modalità di cui al successivo paragrafo, POSSONO indicare dei sub-delegati, con il ruolo di delegati amministrativi o delegati tecnici.

4. Autenticazione degli utenti del Portale

Il rappresentante nominato in fase di perfezionamento dell'accordo di adesione o i sub-delegati indicati nonché gli utenti del Portale, si autenticano digitalmente al Portale con credenziali compatibili con la specifica LoA 3 o superiore dello standard ISO/IEC DIS 29115, scelgono per conto di quale Soggetto erogatore accedono e il ruolo con cui accedono tra quelli ad essi assegnati.

Il Portale PUÒ prevedere una funzione grazie alla quale il Soggetto erogatore e il ruolo con cui accedere per conto di tale Soggetto sono pre-popolati in base all'identità dell'utente.

5. Verifica periodica delle utenze

Il Gestore DEVE assicurare con cadenza periodica la selezione dei Soggetti Erogatori per i quali l'ultima verifica degli utenti è avvenuta oltre l'intervallo di tempo configurato dal Gestore.

Il Gestore DEVE inviare a ognuno dei Soggetti erogatori una comunicazione a mezzo domicilio digitale con l'invito ad accedere al Portale per il tramite dei propri delegati amministrativi e a controllare e, se del caso, rimuovere quei soggetti che non hanno più accesso per conto proprio.

Il Gestore DEVE assicurare con cadenza periodica l'individuazione degli utenti dei Soggetti erogatori il cui comportamento risulti anomalo rispetto alle regole individuate dallo stesso Gestore sulla base delle evidenze determinate dall'utilizzo delle funzionalità messa a disposizione tramite il Portale agli stessi utenti.

Il Gestore DEVE inviare a ognuno dei Soggetti erogatori per cui siano stati individuati utenti di cui al precedente periodo una comunicazione a mezzo domicilio digitale con l'invito a verificare quanto rilevato e, se del caso, accedere al Portale per il tramite dei propri delegati amministrativi e rimuovere gli utenti a cui risulta necessario inibire l'accesso per proprio conto.

6. Configurazione dei Servizi in rete e utilizzo delle API

Il Soggetto erogatore, tramite i suoi delegati tecnici, DEVE assicurare la configurazione dei Servizi in rete e l'utilizzo delle API nel rispetto delle specifiche tecniche di integrazione definite dal Gestore nella Documentazione API.

Allegato 2: Funzionalità del Punto di accesso telematico

1 Identificazione e autenticazione degli utenti finali

L'identificazione dell'utente finale al Punto di accesso telematico DEVE avvenire tramite gli strumenti previsti all'articolo 64 del CAD. A tal fine, il Gestore aderisce alla federazione SPID, previa stipula di apposita convenzione con AgID, e aderisce al sistema CIE secondo la procedura determinata dal Ministero dell'Interno.

Con successive regole tecniche sarà disciplinata anche la possibilità di veicolare l'accesso ai servizi gestiti dai Soggetti erogatori tramite un meccanismo di federated identity (eventualmente anche con modalità single sign-on).

2 Messaggi

La funzione "messaggi" consente all'utente di ricevere le comunicazioni a lui indirizzate da parte del Gestore o dei Soggetti erogatori che utilizzano le API messe a disposizione dal Gestore stesso.

Il Gestore permette all'utente di ordinare e/o filtrare i messaggi ricevuti sulla base di distinti parametri, quali, ad esempio, la data di invio del messaggio, l'identificativo del servizio mittente del messaggio, l'oggetto indicato nel messaggio, etc.

L'utente, se lo desidera, PUÒ attivare ulteriori funzionalità collegate, quali la possibilità di gestire le preferenze di recapito per uno specifico servizio, condividere con terzi il messaggio, ricevere avvisi in merito alla scadenza legata al messaggio (nel caso, per esempio, di avvisi di pagamento), etc.

Il Gestore DEVE consentire ai Soggetti erogatori di interrogare un servizio per sapere se uno specifico utente ha tale servizio attivo sul Punto di accesso telematico e se ha espresso preferenze (per esempio nel caso in cui il cittadino non voglia più ricevere messaggi dall'Ente).

I messaggi POSSONO contenere delle call to action volte, ad esempio, a inserire un "Promemoria" nel proprio calendario personale o un tasto "Paga" per facilitare l'avvio di un flusso

di pagamento. Le Call to Action nei messaggi POSSONO inoltre essere personalizzate dal Soggetto erogatore (es. "Visualizza", "Richiedi", "Iscrivi", etc.) e dare inizio a specifici flussi o azioni dispositive integrate nell'esperienza dell'utente all'interno del Punto di accesso telematico, anche tramite federated identity di cui al paragrafo 1 del presente Allegato.

3 Portafoglio

La sezione "portafoglio", integrata con la piattaforma di cui all'art. 5, comma 2 del CAD ("**Piattaforma PagoPA**"), consente all'utente di pagare un Soggetto erogatore, di salvare e gestire i propri metodi di pagamento e di avere a disposizione la lista delle transazioni eseguite.

Le funzioni di pagamento consentono di eseguire le transazioni economiche all'interno del Punto di accesso telematico, rimanendo nello stesso ambiente e utilizzando i metodi di pagamento già inseriti, portando al completamento dell'operazione in pochi passaggi.

Tutti i dati relativi ai metodi di pagamento e alle transazioni e operazioni di pagamento effettuate vengono mantenuti all'interno della Piattaforma PagoPA nel rispetto delle politiche di data retention individuate in base alle finalità.

Nell'ambito della funzione "portafoglio", il Gestore PUÒ inoltre rendere disponibili servizi specifici legati a bonus e agevolazioni che permettono all'utente finale di gestire tramite il Punto di accesso telematico sia azioni di pagamento sia la ricezione di crediti o l'utilizzo di sistemi di bonus per il pagamento verso terzi.

4 Servizi

La funzione "servizi" permette all'utente finale di verificare in ogni momento quali sono i servizi disponibili all'interno del Punto di accesso telematico e approfondire i dettagli per ciascun servizio.

Ogni servizio è descritto in modo completo, in modo che l'utente sappia cosa aspettarsi da quello specifico servizio all'interno del Punto di accesso telematico. Per la descrizione, il Soggetto erogatore indica per ciascun servizio: il logo, la descrizione dell'offerta di servizi disponibile tramite il Punto di accesso telematico e una serie di metadati necessari per individuare maggiori approfondimenti o mettersi in contatto con il Soggetto erogatore in caso di necessità (la URL dell'informativa privacy, la URL dei termini di servizio, indirizzo fisico, email, eventuale numero di telefono, eventuali altri canali di supporto, etc.).

I servizi POSSONO contenere delle call to action personalizzabili dal Soggetto erogatore, volte a dare inizio a specifici flussi o azioni dispositive integrate nell'esperienza dell'utente all'interno del Punto di accesso telematico, anche tramite federated identity di cui al paragrafo 1 del presente Allegato.

Il Gestore DEVE consentire all'utente un meccanismo di opt-in per l'attivazione dei servizi disponibili nel Punto di accesso telematico, garantendo a tutti gli interessati una scelta libera, esplicita e specifica, nonché un meccanismo di opt-in per l'attivazione della funzionalità di inoltro via e-mail dei messaggi ricevuti nel Punto di accesso telematico.

Il Gestore DEVE propagare notifiche push a contenuto generico (senza cioè alcuna indicazione del mittente, dell'oggetto o del suo contenuto), salvo richiesta degli interessati ovvero l'adozione di misure di protezione del dato che rendano lo stesso illeggibile da parte di soggetti terzi, ivi incluso il gestore del sistema operativo scelto dall'interessato stesso.

5 Profilo

La sezione "profilo" consente all'utente di consultare un riepilogo delle proprie informazioni rilevanti sul Punto di accesso telematico e di impostare alcune scelte di carattere generale che risultano trasversali all'erogazione dei Servizi e che verranno usate per personalizzare il servizio erogato all'utente da parte del Gestore e dei Soggetti erogatori. Alcune di queste scelte, una volta effettuate dall'utente, potranno essere interrogate e utilizzate in tempo reale dai Soggetti erogatori.

Di seguito, si riportano a titolo di esempio alcune preferenze che potranno essere impostate dall'utente:

- lingua preferita;
- e-mail personale dell'utente.

L'eventuale aggiornamento dei dati della sezione profilo, ove modificabili in autonomia dagli interessati nel Punto di accesso telematico, non verrà comunicato agli Identity Provider SPID e avrà effetto solo all'interno del Punto di accesso telematico e dei servizi offerti dai Soggetti erogatori.

Nella stessa sezione "profilo" l'utente PUÒ gestire eventuali strumenti complementari di identificazione e sicurezza quale il PIN o, se abilitati dall'utente sul proprio dispositivo, strumenti di identificazione biometrica.

L'utente potrà inoltre visualizzare uno storico degli accessi e interrompere la sessione attualmente attiva sull'applicazione (logout).

Infine, nella sezione "profilo" l'utente potrà:

- consultare i termini e le condizioni d'uso nonché l'informativa sul trattamento dei dati personali del Punto di accesso telematico;
- gestire le preferenze relative alla configurazione dei Servizi, all'inoltro via email dei Messaggi, alla lingua preferita e al calendario;
- gestire le impostazioni di sicurezza, in particolare il codice di sblocco e il riconoscimento biometrico;
- verificare i dati anagrafici e di contatto utilizzati dal Punto di accesso telematico;
- esercitare il diritto di accesso ai propri dati personali ai sensi dell'art. 15 GDPR nonché il diritto alla cancellazione del proprio account e dei relativi dati personali anche ai sensi dell'art. 17 del GDPR.

-

Allegato 3: Integrazione del Punto di accesso telematico con le piattaforme digitali previste dal CAD e da normative specifiche

Il Punto di accesso telematico DEVE essere integrato con le piattaforme indicate di seguito, anche alla luce dell'articolo 7, comma 01 del CAD.

L'integrazione tra il Punto di accesso telematico e le piattaforme di seguito indicate è realizzata, nel rispetto della normativa in materia di protezione ai dati personali, per dare seguito alle esigenze funzionali espresse dal Soggetto Erogatore in merito ai Servizi in rete di cui lo stesso chiede l'implementazione al Gestore i. Il trattamento dei dati personali che interviene a seguito di tali integrazioni si fonda sulla base giuridica e sulle specifiche finalità individuate dal Soggetto Erogatore, nel rispetto del principio di responsabilizzazione di cui all'articolo 5, paragrafo 2 del GDPR.

Il Gestore e il soggetto titolare delle singole piattaforme convengono sulle modalità tecniche per l'integrazione dei propri sistemi, le quali DEVONO essere conformi alle [LG INTEROP TEC].

1 Piattaforma di cui all'art. 5, comma 2 del CAD

Il Punto di accesso telematico è integrato con la piattaforma di cui al comma 2 dell'articolo 5 del CAD, denominata Piattaforma pagoPA, nella funzione di intermediario tecnologico per i Soggetti erogatori al fine di assicurare quanto disposto ai commi 1 e 2-ter dello stesso articolo 5 in relazione agli obblighi e alle possibilità dei Soggetti erogatori dei Servizi in rete.

L'implementazione dell'integrazione del Punto di accesso telematico con la Piattaforma pagoPA è assicurata nel rispetto delle [LG PAGOPA], delle relative specifiche tecniche e nel rispetto della normativa per la protezione dei dati personali.

2 Piattaforma di cui all'art. 6-bis del CAD

Il Punto di accesso telematico è integrato con la piattaforma di cui al comma 1 dell'articolo 6-bis del CAD, denominata Indice nazionale dei domicili digitali delle imprese e dei professionisti (INI-PEC), al fine di assicurare quanto disposto nell'ultimo periodo del comma 2 dello stesso articolo 6-bis in relazione all'esclusività dei domicili digitali inseriti nell'INI-PEC quali mezzi di comunicazione e notifica alle imprese e ai professionisti.

L'implementazione dell'integrazione del Punto di accesso telematico con INI-PEC, nel rispetto della normativa per la protezione dei dati personali, assicura:

- la verifica da parte del Punto di accesso telematico dei domicili digitali iscritti nell'INI-PEC;
- la consultazione da parte del Punto di accesso telematico degli attributi qualificati dell'identità digitale delle imprese e dei professionisti acquisiti nell'INI-PEC ai fini di quanto previsto dall'articolo 64 del CAD.

3 Piattaforma di cui all'art. 6-ter del CAD

Il Punto di accesso telematico è integrato con la piattaforma di cui al comma 1 dell'articolo 6-ter del CAD, denominata Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA), al fine di assicurare quanto disposto in relazione all'utilizzo dei domicili digitali iscritti in IPA per dare seguito alle comunicazioni per lo scambio di informazioni e l'invio di documenti a tutti gli effetti di legge ai soggetti iscritti nell'IPA.

L'implementazione dell'integrazione del Punto di accesso telematico con IPA, realizzata nei modi previsti dalle [LG IPA] e nel rispetto della normativa per la protezione dei dati personali, assicura:

- la verifica da parte del Punto di accesso telematico dei domicili digitali iscritti nell'IPA;
- la consultazione da parte del Punto di accesso telematico dei dati relativi all'Ente e dei nominativi del legale rappresentante, dei responsabili delle Aree Organizzative Omogenee e delle Unità Organizzative registrati nell'IPA.

4 Piattaforma di cui all'art. 6-quater del CAD

Il Punto di accesso telematico è integrato con la piattaforma di cui al comma 1 dell'articolo 6-quater del CAD, denominata 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), al fine di assicurare quanto disposto dal comma

4 dell'articolo 3-bis del CAD in relazione alle comunicazioni elettroniche aventi valore legale ai sensi dell'articolo 1, comma 1, lettera n-ter del CAD rese per il tramite dei domicili digitali iscritti in INAD.

L'implementazione dell'integrazione del Punto di accesso telematico con INAD, realizzata nei modi previsti dalle [LG INAD] e nel rispetto della normativa per la protezione dei dati personali, assicura:

- la verifica da parte del Punto di accesso telematico dei domicili digitali iscritti nell'INAD;
- la consultazione da parte del Punto di accesso telematico dei dati pubblicati nell'INAD.

5 Piattaforma di cui all'art. 50-ter del CAD

Il Punto di accesso telematico è integrato con la piattaforma di cui al comma 2 dell'articolo 50-ter del CAD, denominata Piattaforma Digitale Nazionale Dati (PDND), quale infrastruttura tecnologica abilitante l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni attraverso le componenti della PDND che assicurano l'accreditamento, l'identificazione e la gestione dei livelli di autorizzazione dei soggetti abilitati ad operare sulla stessa.

L'implementazione dell'integrazione del Punto di accesso telematico con la PDND è realizzata nei modi previsti dalle [LG PDND] indicate al comma 2 dell'articolo 50-ter del CAD e nel rispetto della normativa per la protezione dei dati personali.

6 Piattaforma di cui all'art. 62 del CAD

Il Punto di accesso telematico è integrato con la piattaforma di cui al comma 2 dell'articolo 62 del CAD, denominata Anagrafe nazionale della popolazione residente (ANPR), al fine di assicurare quanto indicato nello stesso articolo 62 in materia di circolarità dei dati anagrafici e di accesso ai dati contenuti in ANPR.

L'implementazione dell'integrazione del Punto di accesso telematico con ANPR è realizzata nelle modalità definite dai decreti del Presidente del Consiglio dei Ministri indicati al comma 6 dell'articolo 62 del CAD, dai decreti del Ministro dell'interno previsti al comma 6-bis dello stesso articolo 62 e nel rispetto della normativa per la protezione dei dati personali.

7 Sistema di cui all'art. 64 del CAD

Il Punto di accesso telematico è integrato con il sistema di cui all'articolo 64 del CAD, denominata Sistema pubblico per la gestione delle identità digitali (SPID), al fine di assicurare

quanto disposto dal comma 2-quater dello stesso articolo 64 in relazione all'identificazione dei soggetti che accedono ai Servizi in rete erogati dalle pubbliche amministrazioni.

L'implementazione dell'integrazione del Punto di accesso telematico con SPID è assicurata nel rispetto delle varie Linee guida concernenti il Sistema pubblico per la gestione delle identità digitali, delle derivanti specifiche tecniche e nel rispetto della normativa per la protezione dei dati personali.

8 Strumenti di identificazione di cui all'art. 66 del CAD

Il Punto di accesso telematico è integrato con lo strumento di identificazione di cui all'articolo 66, comma 1 del CAD, denominato carta d'identità elettronica (CIE), al fine di assicurare quanto disposto dall'articolo 64, comma 2-quater del CAD in relazione l'identificazione dei soggetti che accedono ai Servizi in rete erogati dalle PA.

9 Piattaforma per la notificazione digitale degli atti della pubblica amministrazione di cui all'articolo 1, comma 402, della legge 27 dicembre 2019, n. 160

Il Punto di accesso telematico è integrato con la piattaforma per la notificazione digitale degli atti della pubblica amministrazione di cui all'articolo 1, comma 402, della legge 27 dicembre 2019, n. 160 le cui modalità di funzionamento sono indicate all'articolo 26 del decreto-legge 17 luglio 2020, n. 76, convertito in legge 11 settembre 2020, n. 120, ai fini della notificazione di atti, provvedimenti, avvisi e comunicazioni, in alternativa alle modalità previste da altre disposizioni di legge, anche in materia tributaria da parte delle pubbliche amministrazioni.

Allegato 4: Domain model del Punto di accesso telematico

L'architettura di base prevede i seguenti principali oggetti di dominio.

1 Profilo

Rappresenta il Profilo di un utente finale, cioè le sue preferenze. Nel profilo sono raccolti ad esempio:

- il codice fiscale;
- l'e-mail;
- eventuali preferenze di notifica espresse tramite l'app (ricezione o meno di e-mail o messaggi di notifica).

2 Servizi

Rappresenta i Servizi in rete. Per i singoli Servizi in rete sono raccolte tutte le caratteristiche descrittive del servizio, i riferimenti all'organizzazione e al dipartimento che lo emette, l'eventuale presenza di pagamenti associati al servizio o altra azione da parte dell'utente (compreso il reindirizzamento sui sistemi del Soggetto erogatore, anche tramite federated identity di cui al paragrafo 1 dell'allegato 2).

3 Messaggio

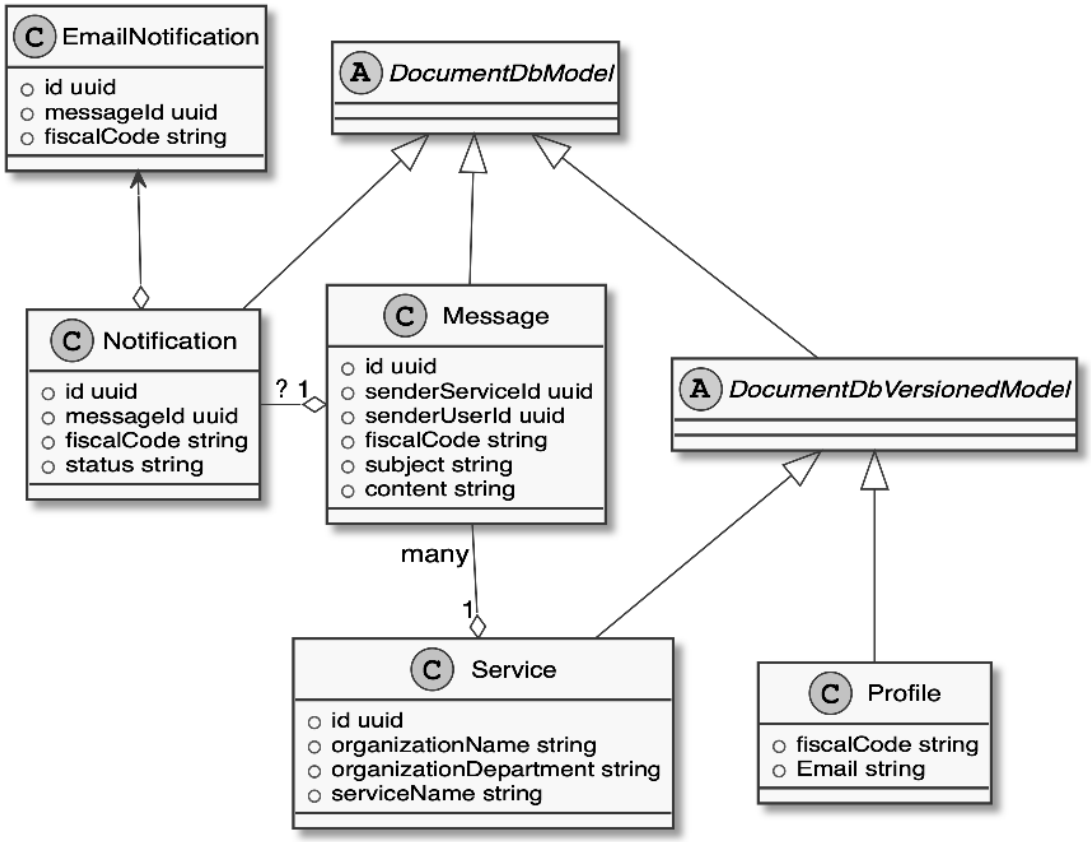
Rappresenta un Messaggio inviato a un utente finale da un Soggetto erogatore in relazione a uno specifico Servizio in rete. Il messaggio può essere di contenuto testuale, avere un link necessario per attivare un relativo pagamento o altra azione da parte dell'utente (compreso il reindirizzamento sui sistemi del Soggetto erogatore, anche tramite federated identity di cui al paragrafo 1 dell'allegato 2).

4 Notifica

Rappresenta una notifica all'utente finale, attivata da un Messaggio. Una notifica è una comunicazione che viene inviata all'utente finale destinatario del Messaggio e che può essere

consegnata su più canali. Le notifiche hanno funzione di invitare l'utente finale alla lettura del relativo messaggio.

Il seguente diagramma Entity Relationship sintetizza il domain model del Punto di accesso telematico.



Allegato 5: Misure minime di sicurezza

1. Obblighi del Gestore

Ferma restando la necessaria predisposizione di ogni misura tecnica e organizzativa adeguata a garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 GDPR e nel rispetto del principio di responsabilizzazione, il Gestore e i Soggetti erogatori DEVONO implementare almeno le misure indicate nel presente Allegato, avendo cura di adottare, nell'erogazione dei Servizi in rete:

a. misure di autenticazione, autorizzazione e istruzione adeguata dei soggetti designati al trattamento dei dati personali ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del Codice privacy, in funzione dei ruoli ricoperti e delle esigenze di accesso;
b. procedure per la verifica periodica della qualità e della coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti designati al trattamento;
c. sistemi di log o sistemi analoghi che consentano di controllare gli accessi ai database e di rilevare anomalie;
d. precise istruzioni consegnate ai soggetti designati al trattamento, prima dello svolgimento delle relative attività.

Il Gestore DEVE provvedere al monitoraggio dell'infrastruttura del Punto di accesso telematico attraverso l'implementazione di:

- Firewall;
- sistema di DDoS Protection;
- Web Application Firewall, Intrusion Prevention / Detection System.

La gestione degli accessi all'infrastruttura DEVE avvenire attraverso l'implementazione almeno delle seguenti misure:

- l'accesso all'infrastruttura del Punto di accesso telematico da parte di soggetti con privilegi di amministratore individuati dal Gestore per la tenuta in esercizio dello stesso Punti di accesso prevede un'autenticazione a due fattori con rilascio di token;
- l'accesso degli utenti delegati dal Soggetto erogatore al Portale prevede un'autenticazione a due fattori con invio di SMS o chiamata a numero di telefonia mobile.

Il Gestore DEVE implementare meccanismi atti a:

- verificare periodicamente l'aggiornamento delle utenze del proprio personale autorizzato e sospendere quelle che non risultano accedere per un intervallo di tempo predeterminato dal Gestore; e
- individuare ed analizzare comportamenti anomali rispetto al normale utilizzo secondo criteri predeterminati dal Gestore.

Le chiamate dei Soggetti erogatori relativamente ai Servizi in rete realizzati per il tramite del Punto di accesso telematico avvengono nel rispetto delle indicazioni presenti nelle [LG INTEROP TEC] e [LG SICUREZZA].

Gli eventi elencati di seguito, che si svolgono sull'infrastruttura, vengono registrati e conservati in appositi log, gestiti dal Gestore nel rispetto della normativa in materia di trattamento di dati personali:

- richieste di accesso a una API da parte di un Soggetto Erogatore per dare seguito a un servizio abilitato sul Punto di accesso telematico;
- richieste di autenticazione mediante SPID (come prescritto dal DPCM 24 ottobre 2014 e dalle relative regolamentazioni in ambito SPID) e CIE e tracciatura delle operazioni svolte;
- accessi degli amministratori di sistema, e conseguente tracciatura delle operazioni svolte;
- accessi dei delegati del Soggetto erogatore al Portale e conseguente tracciatura delle operazioni svolte.

Il Gestore DEVE effettuare periodicamente l'analisi dei rischi, nel rispetto dello standard internazionale ISO 27005. Al fine di garantire una più efficace gestione del rischio, il Gestore DEVE valutare periodicamente le necessarie implementazioni per l'adeguamento dell'infrastruttura ai requisiti della certificazione prevista dallo standard internazionale ISO/IEC 27001:2017.

Il Gestore DEVE sottoporre periodicamente la piattaforma a procedure di vulnerability assessment e penetration test, svolte anche da soggetti terzi, assicurando l'individuazione proattiva di eventuali problematiche di sicurezza e vulnerabilità e le implementazioni di sviluppo necessarie per la loro mitigazione in base al livello di severità, effettuate periodicamente anche tramite:

- Mobile Application Penetration Test, con simulazione dei possibili scenari di attacco a un'applicazione mobile;
- Secure Code Review (SCR) del Punto di accesso telematico;

- API Security Assessment delle API esposte dal Punto di accesso telematico.

2. Obblighi del Soggetto erogatore

Il Soggetto erogatore DEVE implementare almeno le seguenti misure di sicurezza:

- gestione e tracciatura degli accessi ai propri sistemi informatici che interagiscono con il Punto di accesso telematico, con una profondità storica tale da consentire la raccolta e l'analisi di informazioni relative a incidenti e malfunzionamenti anche per finalità diagnostiche; le informazioni così raccolte devono essere leggibili e conservate al fine di essere rese disponibili al Gestore e alle Autorità di controllo, ove richiesto;
- implementazione di sistemi adeguati di controllo, disaccoppiamento e filtraggio tipici dei servizi esposti su rete pubblica;
- configurazioni di sicurezza di sistema avanzate, da adottare sui sistemi che ospitano le applicazioni web;
- verifica periodica dei livelli di sicurezza comprese le attività di analisi dei rischi, vulnerability assessment e penetration testing.

Le misure di sicurezza e le specifiche tecniche sono adottate in ossequio alla normativa in tema di protezione dei dati personali, in conformità alle [LG SICUREZZA], alle best practice del settore e alle specifiche impartite dal Gestore - nella documentazione correlata al rapporto di adesione - nel suo ruolo di titolare del trattamento dei dati personali con riferimento alle attività indicate al 7.1 Trattamenti e ruoli dei soggetti coinvolti delle LG.

Il Gestore e i Soggetti erogatori DEVONO vigilare sull'adeguatezza delle misure e delle specifiche tecniche e procedere alle implementazioni necessarie a mantenere livelli di sicurezza adeguati, nel rispetto del principio di responsabilizzazione di cui all'art. 5, par. 2 GDPR.