Parere all’AgID sullo schema di Linee guida per l’accesso telematico ai servizi della pubblica amministrazione, ai sensi dell’art. 64-bis del d.lgs. 82/2005 - 1° novembre 2021 [9714315]

VEDI ANCHE COMIUNICATO DEL 3 NOVEMBRE 2021

[doc. web n. 9714315]

Parere all’AgID sullo schema di Linee guida per l’accesso telematico ai servizi della pubblica amministrazione, ai sensi dell’art. 64-bis del d.lgs. 82/2005 - 1° novembre 2021

Registro dei provvedimenti
n. 394 del 1° novembre 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l’avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati – di seguito, Regolamento);

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante “Codice in materia di protezione dei dati personali” (di seguito, Codice);

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell’art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Pasquale Stanzione;

PREMESSO

L’Agenzia per l’Italia digitale (di seguito, AgID), con nota inviata in data 26 ottobre 2021, a integrazione di quelle precedentemente inviate in data 3 maggio, 14 giugno e 22 ottobre 2021, ha trasmesso al Garante, ai sensi dell’art. 71 del d.lgs. 7 marzo 2005, n. 82 (di seguito, CAD), lo schema di “Linee guida per accesso telematico ai servizi della Pubblica Amministrazione”, di cui all’art. 64-bis del medesimo CAD.

1. Il quadro normativo

L’art. 64-bis del CAD e ss.mm., recante “Accesso telematico ai servizi della Pubblica

Amministrazione”, prevede che:

> “1. 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, senza nuovi o maggiori oneri per la finanza pubblica.
>
> 1-bis. Al fine di rendere effettivo il diritto di cui all'articolo 7, comma 01, i soggetti di cui all'articolo 2, comma 2, i fornitori di identità digitali e i prestatori dei 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 relative interfacce applicative e, al fine di consentire la verifica del rispetto degli standard e livelli di qualità di cui all'articolo 7, comma 1, adottano gli strumenti di analisi individuati dall'AgID con le Linee guida.
>
> 1-ter. I soggetti di cui all'articolo 2, comma 2, lettera a), rendono fruibili i propri servizi in rete tramite, nel rispetto del principio di neutralità tecnologica, applicazione su dispositivi mobili anche attraverso il punto di accesso telematico di cui al presente articolo, salvo impedimenti di natura tecnologica attestati dalla società di cui all'articolo 8, comma 2 del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12.
>
> 1-quater. I soggetti di cui all'articolo 2, comma 2, lettera a), rendono fruibili tutti i loro servizi anche in modalità digitale e, al fine di attuare il presente articolo, avviano i relativi progetti di trasformazione digitale entro il 28 febbraio 2021.
>
> 1-quinquies. La violazione dell'articolo 64, comma 3-bis e delle disposizioni di cui al presente articolo, costituisce mancato raggiungimento di uno specifico risultato e di un rilevante obiettivo da parte dei dirigenti responsabili delle strutture competenti e comporta la riduzione, non inferiore al 30 per cento della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei dirigenti competenti, oltre al divieto di attribuire premi o incentivi nell'ambito delle medesime strutture.”.

L’art. 7, comma 01, del CAD, richiamato dal comma 1-bis dell’art. 64-bis, al riguardo aggiunge che “chiunque ha diritto di fruire dei servizi erogati dai soggetti di cui all'articolo 2, comma 2, in forma digitale e in modo integrato, tramite gli strumenti telematici messi a disposizione dalle pubbliche amministrazioni e il punto di accesso di cui all'articolo 64-bis, anche attraverso dispositivi mobili”.

La Presidenza del Consiglio dei Ministri – ai sensi dell’art. 8, commi 2 e 3, del d.l. 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla l. 11 febbraio 2019, n. 12 – si avvale, per la progettazione, lo sviluppo, la gestione e l'implementazione del punto di accesso telematico di cui al citato art. 64-bis del CAD, di PagoPA S.p.a. (di seguito, PagoPA o Gestore, società interamente partecipata dallo Stato, ai sensi dell'art. 9 del d.lgs. 19 agosto 2016, n. 175, costituita con decreto del Presidente del Consiglio dei Ministri del 19 giugno 2019), che agisce sulla base degli obiettivi indicati con direttiva adottata dal Presidente del Consiglio dei Ministri.

2. Lo schema di Linee guida in esame

2.1. La struttura e il funzionamento del punto di accesso telematico

Lo schema di Linee guida in esame, che comprende anche 5 allegati, si occupa di definire le modalità di realizzazione e funzionamento del punto di accesso telematico, che è costituito dall’insieme dei sistemi e delle componenti tecnologiche sviluppate e gestite dal Gestore ai sensi dell’art. 64-bis del CAD per consentire ai soggetti di cui all'art. 2, comma 2, del CAD, e a quelli che ritengano di aderirvi previa stipula di apposita convenzione con il Gestore, (di seguito, Soggetti erogatori), di rendere disponibili agli utenti finali i propri servizi (di seguito, Servizi in rete).

Il punto di accesso telematico, reso disponibile tramite un'interfaccia sia in versione mobile che in versione web, rappresenta un canale complementare agli altri canali digitali già utilizzati dai Soggetti erogatori – i quali rimangono titolari del trattamento dei dati personali (par. 3.2 dello schema) – ma il suo utilizzo è comunque obbligatorio, salvo comprovati impedimenti di natura tecnologica e/o organizzativa (par. 3.4 dello schema).

Il punto di accesso telematico si compone delle seguenti componenti architetturali (parr. 5.1, 5.2 e 5.3 dello schema):

> un front-end multicanale (che include un'applicazione per dispositivi mobili e tablet, la c.d. "App IO", e una versione web) dedicato alla fruizione dei servizi da parte degli utenti finali, mediante interfacce applicative (API) che consentono l'interazione con il back-end. L'utente finale può accedere al front-end tramite procedure di autenticazione informatica forte che utilizza SPID o CIE (cfr. all. 2, par. 1, dello schema);
>
> un back-end, che comunica con il front-end e il back office e con i sistemi di terze parti con cui è integrato; è previsto che vengano applicate tecniche di crittografia asimmetrica, ove necessario in relazione alla natura dei dati scambiati dal singolo servizio in rete, al fine di assicurare la riservatezza dei contenuti dei messaggi scambiati tra i sistemi dei Soggetti erogatori e il front-end che transitano per il back-end; in ogni caso è assicurata l'applicazione di adeguati standard di crittografia a livello di canale;
>
> un back office (c.d. portale) dedicato ai Soggetti erogatori, grazie al quale è possibile, tra le altre cose: la registrazione degli stessi Soggetti erogatori al punto di accesso telematico; l'utilizzo, da parte dei Soggetti erogatori, di 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 realizzate dal Gestore.

Il punto di accesso telematico – oltre a offrire una serie di funzionalità standard (messaggi, portafoglio, servizi e profilo), che possono essere anche incrementate in via facoltativa dal Gestore (par. 5.6 e all. 2 dello schema) – assicura l'integrazione con le piattaforme tecnologiche rilevanti per la digitalizzazione dei processi e dei servizi delle pubbliche amministrazioni (ad esempio, la Piattaforma PagoPA, gli indici di domicili digitali INI-PEC, IPA e INAD, e l'ANPR) (par. 5.5 e all. 3 dello schema).

Lo schema in esame disciplina la procedura che i Soggetti erogatori devono seguire per aderire (anche per il tramite di soggetti aggregatori o di partner tecnologici che agiscono per suo conto) al punto di accesso telematico, sottoscrivendo la documentazione contrattuale predisposta dal Gestore, di cui vengono individuati i contenuti essenziali (par. 6.1 e all. 1, par. 1, dello schema).

Con la nota del 22 ottobre 2021, l'Agenzia per l'Italia digitale ha inoltre rappresentato che "con successive regole tecniche, […] provvederà ad approfondire le tematiche collegate alla possibilità di abilitare sessioni di utenza della durata massima di 30 giorni e consentire l'implementazione del single sign-on, ponendo particolare attenzione ai profili di sicurezza e alle responsabilità delle parti coinvolte".

2.2. Le previsioni in materia di protezione dei dati personali

Il capitolo 7 dello schema si occupa di definire alcuni aspetti relativi alla protezione dei dati personali trattati nell'ambito del punto di accesso telematico. In particolare, con riferimento ai ruoli assunti dai soggetti coinvolti nel trattamento, lo schema stabilisce che (par. 7.1):

> il Gestore è titolare dei trattamenti necessari a:
>
> > a) la progettazione, lo sviluppo, la gestione e l'implementazione del punto di accesso

telematico, ivi incluse le attività volte a permettere l'interoperabilità con le piattaforme abilitanti, nonché quelle di assistenza, debugging e diagnostica, monitoraggio del funzionamento, miglioramento ed evoluzione dello stesso;

b) la realizzazione delle funzionalità e/o dei servizi resi direttamente dal Gestore su richiesta dell'utente finale, ivi incluse le attività finalizzate alla gestione in modo agevole e dinamico della propria relazione con i Soggetti erogatori per i servizi erogati;

c) lo svolgimento di altre attività che gli sono attribuite ai sensi di legge per l'esecuzione di compiti di interesse pubblico;

i Soggetti erogatori agiscono come titolari in relazione ai trattamenti effettuati nell'ambito dei Servizi in rete resi disponibili tramite il punto di accesso telematico (tranne quando, in qualità di Soggetti aggregatori, sono responsabili del trattamento per conto di altre amministrazioni) e il Gestore agisce in qualità di responsabile del trattamento (o, se del caso, di sub-responsabile del trattamento) per conto degli stessi, sulla base di un accordo ai sensi dell'art. 28 del Regolamento.

Più in generale, lo schema individua misure volte ad assicurare il rispetto dei principi di minimizzazione dei dati, di limitazione della conservazione, di liceità, correttezza e trasparenza del trattamento, nonché l'esercizio dei diritti da parte degli interessati (parr. 7.4.1, 7.4.2 e 7.4.4 dello schema), specificando, altresì, che le comunicazioni di dati personali diversi da quelli di cui agli artt. 9 e 10 del Regolamento devono essere effettuate anche nel rispetto dell'art. 2-ter del Codice (par. 7.1 dello schema).

Inoltre, considerato che tramite il punto di accesso telematico potrebbero essere trattate anche categorie di dati personali di cui agli artt. 9 e 10 del Regolamento, è previsto che, in questi casi, siano adottate misure appropriate e specifiche per tutelare i diritti fondamentali e le libertà dell'interessato. L'invio di eventuali messaggi contenenti tali categorie particolari di dati personali deve essere richiesto 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 (par. 7.3 dello schema).

Il Gestore e i Soggetti erogatori sono chiamati a implementare le misure di sicurezza indicate nello schema (spec. all. 5), ferma restando la necessaria predisposizione di ogni misura tecnica e organizzativa adeguata a garantire un livello di sicurezza adeguato al rischio, ai sensi degli artt. 5, parr. 1, lett. f), e 2, e 32 del Regolamento. In ossequio ai principi di privacy 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 tecniche e organizzative aggiuntive rispetto a quanto previsto nell'accordo stipulato ai sensi dell'art. 28 del Regolamento (parr. 7.2 e 7.5 dello schema).

Il Gestore può avvalersi di propri responsabili del trattamento, ai sensi dell'art. 28 del Regolamento, che deve indicare in un elenco da mettere a disposizione dei Soggetti erogatori. Nella scelta dei fornitori, il Gestore deve privilegiare, a parità di garanzie in materia di protezione dei dati personali, coloro che sono situati sul territorio nazionale e dell'Unione europea, in ogni caso istruendoli sulla necessità di conservare i dati all'interno dell'Unione stessa. Laddove ciò non fosse possibile, il Gestore può ricorrere a responsabili situati in Paesi terzi, richiedendo, ove possibile, l'implementazione di misure supplementari al fine di impedire l'identificazione dell'interessato da parte del responsabile e/o da autorità governative straniere. In generale, il Gestore è in ogni caso tenuto a rispettare le misure previste dal capo V del Regolamento, ponendo in essere le misure contrattuali necessarie anche per conto dei Soggetti erogatori (par. 7.4.5 dello schema).

Infine, il Gestore è tenuto a predisporre una valutazione di impatto sulla protezione dei dati da sottoporre a consultazione del Garante, e da mettere a disposizione dei Soggetti erogatori come ausilio alla valutazione d'impatto che gli stessi dovranno eventualmente sottoporre al Garante in caso di trattamenti caratterizzati da un rischio elevato in assenza di misure adottate per attenuare tale rischio (artt. 35 e 36, par. 1, del Regolamento).

OSSERVA

Lo schema di Linee guida in esame tiene conto delle indicazioni fornite dall'Ufficio, nel corso delle numerose interlocuzioni tenutesi con i rappresentati dell'Agenzia per l'Italia digitale e di PagoPA, volte a individuare opportune garanzie per assicurare la conformità al Regolamento e al Codice dei trattamenti dei dati personali effettuati nell'ambito del punto di accesso telematico, con particolare riferimento ai seguenti aspetti:

i ruoli assunti nel trattamento dal Gestore e dai Soggetti erogatori (par. 7.1 dello schema), nonché dai soggetti aggregatori e dai partner tecnologici (parr. 6.1.2 e 6.1.3 dello schema), al fine di assicurare il rispetto dei principi di liceità, correttezza e trasparenza e di limitazione della finalità di cui all'art. 5, par. 1, lett. a) e b), del Regolamento;

la descrizione delle attività di trattamento poste in essere nell'ambito del punto di accesso telematico, in ossequio al principio di liceità, correttezza e trasparenza di cui all'art. 5, par. 1, lett. a), del Regolamento;

le modalità di adesione al punto di accesso telematico da parte dei Soggetti erogatori, definendo anche i contenuti degli accordi di adesione (par. 6.1 e all. 1 dello schema), in conformità agli artt. 24 e 28 del Regolamento;

le garanzie da adottare in caso di trattamenti di categorie particolari di dati personali, di cui all'art. 9 del Regolamento, o di dati relativi a condanne penali e reati, di cui all'art. 10 del medesimo Regolamento (par. 7.3 dello schema);

le responsabilità del Gestore e dei Soggetti erogatori nella valutazione dei rischi derivanti dai trattamenti effettuati, da effettuarsi anche ai sensi degli artt. 35 e 36 del Regolamento (par. 7.4.3 dello schema);

le garanzie che il Gestore deve assicurare in caso di riscorso a responsabili del trattamento (par. 7.4.5 dello schema);

le misure volte ad assicurare un livello di sicurezza adeguato ai rischi presentati dal trattamento (par. 7.5 e all. 5 dello schema), con particolare riguardo al tracciamento delle interazioni con le altre piattaforme, nonché degli accessi e delle operazioni compiute dai soggetti autorizzati (parr. 5.5 e 7.5.5 dello schema), in ossequio al principio di integrità e riservatezza e nel rispetto degli obblighi in materia di sicurezza di cui agli artt. 5, par. 1, lett. f), e 32 del Regolamento;

il trattamento dei dati di contatto degli utenti, da effettuarsi nel rispetto dei principi di liceità, correttezza e trasparenza, di minimizzazione dei dati e di esattezza di cui all'art. 5, par. 1, lett. a), c) e d), del Regolamento;

l'individuazione di misure volte ad agevolare l'esercizio dei diritti da parte degli interessati, nel rispetto degli artt. 12 e ss. del Regolamento (all. 2, par. 5, dello schema);

le modalità di integrazione del punto di accesso telematico con le piattaforme digitali previste dal CAD e da altre normative specifiche, nel rispetto dei principi di liceità, correttezza e trasparenza e di limitazione della finalità di cui all'art. 5, par. 1, lett. a) e b), del Regolamento

(all. 3 dello schema);

le garanzie e le misure da adottare, nell'ambito dell'App IO, per l'utilizzo di sessioni utente di lunga durata, a seguito di autenticazione informatica tramite SPID o CIE, e per l'accesso ai servizi gestiti dai Soggetti erogatori tramite un meccanismo di federated identity (eventualmente anche con modalità single sign-on), che saranno individuate dall'AgID nell'ambito di apposite regole tecniche (all. 2, par. 1, dello schema).

RITENUTO

Lo schema di Linee guida in esame disciplina, ai sensi dell'art. 64-bis del CAD, i trattamenti effettuati nell'ambito del punto di accesso telematico ai servizi della pubblica amministrazione, necessari per l'esecuzione di un compito di interesse pubblico, nel rispetto di quanto previsto dall'art. 6, parr. 1, lett. e), e 3, del Regolamento, nonché dall'art. 2-ter del Codice.

Al riguardo, si osserva che il predetto schema, che tiene conto delle indicazioni fornite dall'Ufficio sopra descritte, risulta conforme ai principi stabiliti in materia di protezione dei dati personali dal Regolamento e dal Codice, e, pertanto, con il presente provvedimento, reso ai sensi degli artt. 36, par. 4, e 57, par. 1, lett. c), del Regolamento, si esprime parere favorevole.

L'analisi delle ulteriori misure che verranno adottate dal Gestore per mitigare i rischi elevati presentati dal trattamento sarà effettuata nell'ambito dell'esame della valutazione di impatto sulla protezione dei dati, che sarà trasmessa da PagoPA al Garante (cfr. par. 7.4.3 dello schema); ciò, fermo restando quanto già stabilito dal Garante con i precedenti provvedimenti relativi ai trattamenti di dati personali effettuati mediante l'App IO (cfr., in particolare, il provv. n. 230 del 9 giugno 2021, doc. web n. 9668051, e il provv. n. 242 del 16 giugno 2021, doc. web n. 9670061).

Infine, con riferimento alla possibilità di ricorrere a responsabili del trattamento stabiliti in Paesi terzi, si ricorda che l'esportatore, in caso di utilizzo di uno degli strumenti previsti dall'art. 46 del Regolamento per assicurare un livello di protezione adeguato ai dati trasferiti (ad esempio, le clausole contrattuali standard adottate dalla Commissione europea), è comunque tenuto a verificare se la legge o la prassi del Paese terzo in cui si trasferiscono i dati permettono alle autorità pubbliche locali ingerenze nei diritti delle persone interessate che vadano oltre quanto strettamente necessario per conseguire l'obiettivo legittimo perseguito e non esista contro tali ingerenze una tutela giuridica efficace. In tal caso, l'esportatore è tenuto ad adottare misure supplementari che garantiscano il rispetto delle garanzie contenute negli strumenti utilizzati e quindi un livello di protezione dei dati personali sostanzialmente equivalente a quello previsto dal Regolamento (cfr. le "Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE", adottate dal Comitato europeo per la protezione dei dati il 10 novembre 2020).

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi degli artt. 36, par. 4, e 57, par. 1, lett. c), del Regolamento, esprime parere favorevole sullo schema di "Linee guida per accesso telematico ai servizi della Pubblica Amministrazione" di cui all'art. 64-bis del d.lgs. 7 marzo 2005, n. 82, predisposto dall'Agenzia per l'Italia digitale ai sensi dell'art. 71 del medesimo d.lgs. 7 marzo 2005, n. 82.

Roma, 1° novembre 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei