GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 3953181]

Parere su uno schema di regolamento recante le modalità per l'accreditamento e la vigilanza sui gestori dell'identità digitale - 23 aprile 2015

Registro dei provvedimenti
n. 238 del 23 aprile 2015

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano, componente e del dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere dell'Agenzia per l'Italia digitale;

Visto l'articolo 154, comma 4, del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

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

Relatore il dott. Antonello Soro;

PREMESSO

1. L'Agenzia per l'Italia digitale (di seguito AGID o Agenzia) ha richiesto il parere del Garante su uno schema di regolamento recante le modalità per l'accreditamento e la vigilanza sui gestori dell'identità digitale.

Il regolamento è adottato ai sensi dell'articolo 4, comma 3, del decreto del Presidente del Consiglio dei ministri 24 ottobre 2014 (di seguito dPCM) recante la 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 da parte delle pubbliche amministrazioni e delle imprese, sul cui schema il Garante ha reso parere in data 19 giugno 2014.
L'articolo 4 del dPCM, infatti, ai commi 2, 3 e 4, prevede che l'Agenzia adotti regolamenti per definire le regole tecniche e le modalità attuative per la realizzazione dello SPID, le modalità di accreditamento dei soggetti SPID, nonché le procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale. Con tali regolamenti devono essere disciplinati anche altri profili, richiamati in altri articoli del decreto.

Anche gli schemi degli altri provvedimenti sono stati trasmessi al Garante e su di essi l'Autorità si esprimerà con separato parere.

RILEVATO

2. Occorre premettere che lo SPID consente agli "utenti" (persone fisiche o giuridiche che utilizzano i servizi erogati in rete) di avvalersi di specifici soggetti, i "gestori dell'identità digitale", per consentire ai "fornitori di servizi" l'immediata verifica della propria identità e di eventuali "attributi qualificati" che li riguardano (art. 2 dPCM).

I soggetti pubblici o privati che partecipano allo SPID sono: i gestori dell'identità digitale ("le persone giuridiche accreditate allo SPID che, in qualità di gestori di servizio pubblico, previa identificazione certa dell'utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Essi inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti"); i "gestori degli attributi qualificati"; i fornitori di servizi (definiti quali fornitori dei servizi della società dell'informazione, ex art. 2, comma 1, lett. a), d. lg. n. n. 70/2003 o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili al pubblico); l'Agenzia per l'Italia digitale e gli utenti. Tali soggetti, eccettuati gli utenti, costituiscono un sistema aperto e cooperante che consente loro di comunicare utilizzando meccanismi di interazione, standard tecnologici e protocolli indicati nel decreto e dettagliati nelle regole tecniche definite dall'Agenzia con proprio regolamento (art. 3 dPCM).

Per "identità digitale" si intende la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale (art. 1, comma 1, lett. o)). Premesso che per "attributi" si intendono le informazioni o la qualità di un utente utilizzate per rappresentare la sua identità, il suo stato, la sua forma giuridica o altre caratteristiche peculiari, lo schema distingue fra: "attributi identificativi" (nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché il codice fiscale e gli estremi del documento d'identità utilizzato ai fini dell'identificazione); "attributi non identificativi" (il numero di telefonia mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché eventuali altri attributi individuati dall'Agenzia); "attributi qualificati" (le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi

altro tipo di attributo attestato da un gestore di attributi qualificati) (art. 1, comma 1, lett. a), b), c) e d)).

Le identità digitali rilasciate all'utente contengono obbligatoriamente il "codice identificativo" e gli attributi identificativi e possono contenere gli attributi non identificativi, gli attributi qualificati e ulteriori attributi registrati su richiesta dell'utente nell'ambito delle categorie individuate dall'Agenzia tramite i regolamenti di cui all'articolo 4.

Gli articoli 10, 11 e 12 del dPCM disciplinano la procedura di accreditamento dei gestori dell'identità digitale, gli obblighi previsti in capo ad essi in relazione al funzionamento dello SPID, nonché la cessazione, sospensione e revoca della loro attività.

3. Tutto ciò premesso, il regolamento si compone di 8 paragrafi e di un allegato, parte integrante del regolamento, che riporta la documentazione necessaria per l'accreditamento, da allegare alla domanda.

Il paragrafo 1 individua i requisiti per l'accreditamento dei gestori.

In particolare si prevede che tali soggetti debbano:

a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere l'attività di gestore di identità digitale nell'ambito dello SPID;

b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del CAD e le regole tecniche previste;

c) essere titolari di certificazione UNI EN ISO 9001 e ISO/IEC 27001 nelle edizioni applicabili e metodi e tecniche amministrative consolidate per la realizzazione dei servizi SPID di cui al DPCM;

d) adottare adeguate misure di protezione idonee a garantire la riservatezza, l'autenticità, l'immodificabilità, l'integrità dei dati e la fruibilità dei servizi.

Il gestore, se soggetto privato, in aggiunta a quanto previsto dai precedenti punti, deve inoltre garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche.

Il paragrafo 1 descrive poi gli effetti dell'accreditamento e le attività di vigilanza dell'AGID (per queste ultime, v. anche par. 7).

I gestori che conseguono l'accreditamento e che stipulano la prevista convenzione con l'AGID (art.10 comma 2 dPCM) sono iscritti nel "registro SPID" (art. 1 comma 1, lett. s), dPCM), come soggetti abilitati ad operare in qualità di gestori di identità digitale.

Sui soggetti accreditati l'Agenzia esercita attività di vigilanza, volta ad assicurare che siano mantenuti nel tempo i requisiti che hanno consentito l'iscrizione, pena la revoca dell'accreditamento e la conseguente cancellazione dal registro.

Il gestore per il quale sia stato disposto un provvedimento di revoca non può presentare una nuova domanda di accreditamento se non siano cessate le cause che hanno dato luogo alla cancellazione dall'elenco e, in ogni caso, non prima che siano trascorsi 6 mesi dall'emissione del provvedimento di revoca.

Per espletare le attività per l'accreditamento dei gestori e per svolgere le connesse funzioni di vigilanza, l'Agenzia si avvale di apposita struttura, istituita nell'ambito delle proprie dotazioni organiche. Essa si riserva di verificare, anche a campione, il rispetto delle Norme ISO/IEC 27001, avvalendosi di terze parti accreditate dall'Ente Unico di Accreditamento Nazionale.

Gli articoli 2 e 3 disciplinano la presentazione della domanda di accreditamento, cui devono essere allegati una serie di documenti espressamente indicati nell'allegato al regolamento, e l'iter istruttorio della domanda di accreditamento.
La domanda di accreditamento è predisposta in formato elettronico, o fornita in copia ai sensi dell'art. 22, comma 2, del CAD, sottoscritta con firma digitale o firma elettronica qualificata dal legale rappresentante del richiedente; con le medesime modalità deve essere predisposta la documentazione per l'accreditamento.

Seguono poi gli elementi che deve contenere la domanda, fra cui si evidenzia l'indicazione del "referente per la protezione dei dati personali".

L'allegato al regolamento descrive i documenti che devono essere presentati unitamente alla domanda, fra i quali assume particolare importanza il "piano per la sicurezza", che deve attenersi alle misure di sicurezza previste dal Codice.

L'Agenzia nel corso dell'istruttoria può effettuare verifiche sulla rispondenza dei protocolli di autenticazione a quanto previsto dalla regole tecniche e prove sull'adeguatezza e l'usabilità delle soluzioni tecnologiche di autenticazione informatica.

Al termine dell'istruttoria, l'Agenzia accoglie la domanda ovvero la respinge con provvedimento motivato e ne dà apposita comunicazione al richiedente. Il soggetto la cui domanda sia stata respinta, non può presentare una nuova domanda se non siano cessate le cause che hanno determinato il mancato accoglimento della precedente e, comunque, non prima che siano trascorsi sei mesi dalla data di deposito della domanda respinta.

Come anticipato sopra, a seguito dell'accreditamento, l'Agenzia informa il richiedente ai fini della sottoscrizione della prevista convenzione (par. 4 dello schema) e a seguito della avvenuta stipula l'AGID dispone l'iscrizione del gestore di identità nell'apposito registro SPID, i cui contenuti sono disciplinati al successivo paragrafo 5.

Il gestore di identità accreditato, ottenuta l'iscrizione nell'apposito registro, può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni e, opportunamente, per finalità di trasparenza, deve pubblicare in una sezione del proprio sito web, denominata "soluzioni tecnologiche per l'autenticazione SPID" almeno l'elenco delle soluzioni di autenticazione approvate dall'Agenzia con livello di sicurezza associato e la relativa data di approvazione.

Particolarmente importante è il paragrafo 6 che disciplina l'iter di valutazione e autorizzazione da parte dell'AGID delle soluzioni tecnologiche utilizzabili nel sistema SPID in relazione ai diversi livelli di sicurezza ammessi.

Occorre infatti considerare che l'articolo 6 del dPCM disciplina i livelli di sicurezza delle identità digitali sancendo che lo SPID è basato su tre livelli di sicurezza di "autenticazione informatica". L'Agenzia valuta e autorizza l'uso degli strumenti e delle tecnologie di autenticazione informatica consentiti per ciascun livello, nonché i criteri per la valutazione dei sistemi di autenticazione informatica e la loro assegnazione al relativo livello di sicurezza. In tale ambito, i gestori dell'identità digitale rendono pubbliche le decisioni dell'Agenzia con le modalità indicate dalla stessa.

Lo schema prevede che la domanda, da presentarsi all'AGID, debba recare in allegato il "rapporto di conformità" della soluzione tecnologica prospettata (v. par. 8) e altra documentazione utile a comprovare la sussistenza dei requisiti tecnici necessari.

Per quanto riguarda il "rapporto di conformità" (par. 8), tale documento è rilasciato da enti di certificazione accreditati dall'Ente Unico di Accreditamento Nazionale, istituito in attuazione del Regolamento UE 765/2008 e riconosciuto in uno dei Paesi dell'Unione Europea.

A tal riguardo, l'AGID entro il 30 giugno 2015 dovrà predisporre le norme tecniche e i criteri di accreditamento ed individuazione degli enti di certificazione, finalizzati alla valutazione di conformità dei sistemi di autenticazione informatica ai livelli di sicurezza di cui all'articolo 6 del dPCM.

I soggetti che presentano domanda di accreditamento dell'identità digitale sottopongono i propri sistemi di autenticazione informatica alla valutazione dei predetti Enti e una volta ottenuto il rapporto di conformità, lo trasmettono all'Agenzia.

Lo schema di regolamento prevede che, in sede di prima applicazione, e nelle more della predisposizione delle norme tecniche e dei criteri di accreditamento sopra citati, i soggetti siano tenuti ad allegare alla domanda di valutazione di cui al paragrafo 6, in luogo del previsto rapporto di conformità, una relazione tecnica dettagliata che evidenzi il livello di sicurezza del sistema di autenticazione informatica, e a sottoporre i propri sistemi di autenticazione informatica alla valutazione entro il termine massimo di quattro mesi dalla data di accreditamento del secondo ente di certificazione.

L'Agenzia può effettuare verifiche sulla rispondenza dei sistemi di autenticazione informatica a quanto previsto dalla regole tecniche e a tal fine, i richiedenti, fin dalla presentazione della domanda di accreditamento, mettono a disposizione dell'Agenzia un ambiente di prova per le verifiche.

L'Agenzia, ai sensi del comma 2 dell'articolo 6 del dPCM, esamina la documentazione presentata e l'esito degli eventuali test effettuati e, tenuto conto del rapporto di conformità o della relazione tecnica di cui al successivo paragrafo 8, valuta la sicurezza della soluzione di autenticazione informatica assegnando il relativo livello di sicurezza.

L'esito di tale valutazione è comunicato formalmente dall'Agenzia al richiedente che, qualora decida di accettarlo, trasmette comunicazione in tal senso all'Agenzia allegando copia del manuale operativo e del piano della sicurezza aggiornati.

I richiedenti si conformano alle valutazioni dell'AGID pena l'adozione dei provvedimenti di cui all'articolo 12 del dPCM (sospensione, revoca, ecc.).

RITENUTO

4. Il Garante annette particolare importanza alla materia in esame, in ragione della delicatezza dei trattamenti di dati personali previsti, specialmente sotto il profilo dei rischi di furto, uso abusivo, o alterazione dell'identità degli interessati e del necessario elevato grado di sicurezza dei dati e dei sistemi.

Per tali motivi, lo schema di regolamento è stato elaborato dall'AGID all'esito di numerose riunioni e interlocuzioni avute con l'Ufficio del Garante il quale ha formulato rilievi e ha fornito indicazioni volte a perfezionare il testo e a renderlo pienamente conforme alla disciplina in materia di protezione dei dati personali; le indicazioni sono state accolte dall'Agenzia anche attraverso una nuova formulazione di alcuni paragrafi.

Le indicazioni rese dall'Ufficio hanno riguardato, in particolare:

a) un più puntuale coordinamento con la normativa di settore, e in particolare con il decreto del 2014 cui si intende dare attuazione;

b) l'indicazione, tra i soggetti di cui all'articolo 10, comma 3, lett. e), del dPCM, del "referente per la protezione dei dati personali", figura che assume particolare rilevanza ai fini del rispetto della normativa in materia e dell'esercizio dei controlli da parte del Garante (par. 2, punto 7, lett. g)). A tal riguardo, il Garante auspica che ogni titolare coinvolto dall'applicazione del presente

regolamento individui al suo interno una figura di referente della protezione dei dati che interloquisca con l'Autorità, anche in relazione ai casi di data breach (art. 11, comma 1, lett. o), dPCM);

c) l'integrazione dell'attività di vigilanza dell'AGID con riferimento agli aspetti di collaborazione con il Garante. Il paragrafo 7 riporta, infatti, ora la previsione secondo cui l'AGID informa il Garante di possibili violazioni della normativa in materia di protezione dei dati personali evidenziatesi nel corso della vigilanza;

d) il rafforzamento e la razionalizzazione delle misure a protezione dei dati e dei sistemi, al fine di garantire un elevato livello di sicurezza, adeguato all'estrema delicatezza dei trattamenti. In particolare, è stato descritto nel dettaglio il processo di accreditamento e l'attività di vigilanza svolta dall'Agenzia nei confronti dei gestori accreditati, nonché i requisiti formativi e curriculari delle figure professionali con responsabilità in attività connesse alla sicurezza, alla conduzione dei sistemi, alle verifiche e ispezioni, alla formazione del personale, alla conservazione della documentazione;

e) una più puntuale descrizione del processo di approvazione delle soluzioni tecnologiche per l'autenticazione informatica, con particolare riguardo all'individuazione delle diverse fasi, alla documentazione presentata, alle prove tecniche necessarie e all'attività di valutazione posta in capo all'Agenzia.

5. Nondimeno, in ragione della complessità e dell'importanza della materia, resta l'esigenza di apportare al provvedimento alcuni perfezionamenti, nei termini di seguito descritti.

5.1. Al paragrafo 1 del regolamento, è necessario integrare il punto 2 relativo alle competenze richieste al personale dei gestori dell'identità digitale, con la previsione del requisito di una specifica conoscenza nel settore della protezione dei dati personali.

5.2. Nello stesso paragrafo 1, occorre integrare gli obblighi in capo ai gestori per i quali sia stato disposto dall'Agenzia un provvedimento di revoca, ai fini di minimizzare i rischi di un uso delle identità rilasciate non conforme ai requisiti stabiliti dal dPCM, i cui effetti potrebbero arrecare pregiudizio non solo ai titolari delle stesse identità, ma anche al livello di fiducia e di sicurezza dell'intero sistema SPID. In particolare, si suggerisce di prevedere che, in tal caso, il gestore destinatario del provvedimento di revoca provveda, entro le 12 ore successive dall'avvenuta conoscenza del provvedimento, alla sospensione del servizio di identificazione elettronica dandone contestuale comunicazione agli utenti.

5.3. Al medesimo paragrafo 1, il regolamento prevede che l'Agenzia "per espletare le attività per l'accreditamento dei gestori e per svolgere le connesse funzioni di vigilanza" possa avvalersi "di apposita struttura, istituita nell'ambito delle proprie dotazioni organiche". Tale previsione va coordinata con quanto indicato nel paragrafo 7 dello stesso Regolamento, in cui si indica la possibilità che l'esecuzione delle verifiche ispettive possa essere demandata dall'Agenzia a soggetti terzi.

5.4. Al paragrafo 7, l'ultimo capoverso va perfezionato sostituendo le parole: "dei regolamenti" con "della normativa".

5.5. Nell'allegato al regolamento, che contiene l'elenco della documentazione da allegare alla domanda di accreditamento, alla lettera s) del paragrafo 2 occorre dare maggiore evidenza alle misure adottate ai fini della protezione dei dati e dei sistemi. Si propone pertanto di sostituire il testo con il seguente: "s) copia del piano per la sicurezza, redatto in conformità con quanto disposto al paragrafo 3, che evidenzi in particolare le idonee misure di sicurezza adottate, ai sensi dell'articolo 31 del Codice, rispetto ai rischi di distruzione o perdita dei dati personali, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di furto, uso abusivo, o alterazione di identità, nonché di ripudio o disconoscimento di una transazione. Il piano deve essere cifrato con la chiave pubblica resa disponibile dall'Agenzia".

Per le medesime finalità, occorre altresì sostituire la lettera t) dello stesso paragrafo con la seguente "t) relazione che descrive i trattamenti di dati personali effettuati riportandone le informazioni essenziali e le misure messe in atto per conformare tali trattamenti alla normativa sulla protezione dei dati personali, con particolare riferimento ai principi di necessità, pertinenza e non eccedenza dei dati, nonché di correttezza del trattamento e all'obbligo di rendere previa e idonea informativa agli utenti del servizio di identificazione elettronica".

IL GARANTE

esprime parere favorevole sullo schema di regolamento dell'Agenzia per l'Italia digitale recante le modalità per l'accreditamento e la vigilanza sui gestori dell'identità digitale, con le seguenti condizioni:

a) al paragrafo 1 del regolamento, si integri il punto 2 con la previsione del requisito di una specifica conoscenza nel settore della protezione dei dati personali (punto 5.1.);

b) al medesimo paragrafo 1, si preveda che il gestore destinatario del provvedimento di revoca provveda, entro le 12 ore successive dall'avvenuta conoscenza del provvedimento, alla sospensione del servizio di identificazione elettronica dandone contestuale comunicazione agli utenti (punto 5.2.).

c) sempre al paragrafo 1, la previsione che l'Agenzia "per espletare le attività per l'accreditamento dei gestori e per svolgere le connesse funzioni di vigilanza" possa avvalersi "di apposita struttura, istituita nell'ambito delle proprie dotazioni organiche" sia coordinata con quanto indicato nel paragrafo 7, nei termini di cui in motivazione (punto 5.3.);

d) al paragrafo 7, ultimo capoverso, le parole: "dei regolamenti" siano sostituite dalle seguenti: "della normativa";

e) all'allegato al regolamento, siano apportate le modifiche di cui al punto 5.5.

Roma, 23 aprile 2015

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia