Parere sullo schema di Linee guida di design per i siti internet e i servizi digitali della PA, predisposto dall'AgID - 24 febbraio 2022 [9753209]

VEDI ANCHE Newsletter del 14 marzo 2022

[doc. web n. 9753209]

Parere sullo schema di Linee guida di design per i siti internet e i servizi digitali della PA, predisposto dall'AgID - 24 febbraio 2022

Registro dei provvedimenti
n. 76 del 24 febbraio 2022

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, l'avv. Guido Scorza, componente 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 d.lgs. 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 l'avv. Guido Scorza;

PREMESSO

L'Agenzia per l'Italia Digitale (di seguito, AgID), con nota del 5 luglio 2021, ha sottoposto al Garante, ai sensi dell'art. 71, comma 1, del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale – di seguito, CAD), lo schema di "Linee guida di design per i siti internet e i servizi digitali della PA", contenenti regole che, in attuazione dell'art. 53, comma 1-ter, del CAD, definiscono "le modalità per la realizzazione e la modifica dei siti delle amministrazioni".

Lo schema di linee guida, che tiene conto degli esiti della consultazione pubblica effettuata dall'AgID, annulla e sostituisce le precedenti "Linee guida per i siti web delle PA" di cui all'art. 4 della Direttiva del Ministro per la pubblica amministrazione e l'innovazione del 26 novembre 2009, n. 8.

I destinatari dello schema in esame, secondo quanto previsto dal paragrafo 2.2, sono le pubbliche amministrazioni, così come definite nell'art. 2, comma 2, lett. a), del CAD.

Lo scopo del documento, come chiarito nel paragrafo 2.1, è individuato nella necessità di "definire e orientare la progettazione e la realizzazione dei siti internet e servizi digitali erogati dalle Pubbliche Amministrazioni".

Lo schema di linee guida, oltre ai pertinenti riferimenti normativi (paragrafo 3.1), sintetizza, in particolare, le azioni che le pubbliche amministrazioni devono (o dovrebbero) compiere al fine di:

rendere accessibili a tutti gli utenti i siti web e i servizi digitali delle pubbliche amministrazioni, nel rispetto dei requisiti di legge (paragrafo 5.1 - "Accessibilità");

assicurare la sicurezza dei siti web e dei servizi digitali, nel rispetto del Regolamento e del Codice (paragrafo 5.2 - "Affidabilità e sicurezza"), ponendo in essere le seguenti azioni:

a) "garantire la protezione dei dati personali, nello sviluppo di un sito web o di un servizio digitale, fin dalla progettazione e per impostazione predefinita, nel rispetto dell'art. 25 del GDPR";

b) "rispettare almeno il livello base di sicurezza stabilito dalle «Misure minime di sicurezza ICT per le pubbliche amministrazioni», ove non sia specificamente richiesto un livello superiore dal citato documento";

c) "porre in atto misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio, nel rispetto di quanto richiesto all'art. 32 del GDPR e in ottica di responsabilizzazione ai sensi dell'art. 5, par. 2 del GDPR";

d) "pubblicare, sul singolo sito, l'informativa sul trattamento dei dati personali e chiedere il consenso laddove necessario, anche con riferimento all'uso dei cookie";

e) "provvedere a inserire i trattamenti di dati personali nel Registro dei trattamenti e nominare Responsabili del trattamento ai sensi dell'art. 28 del GDPR gli eventuali fornitori dei servizi web che trattano dati personali per conto del soggetto titolare del trattamento";

analizzare e migliorare l'esperienza d'uso dei siti web e dei servizi digitali mediante la rilevazione qualitativa e quantitativa dei dati di fruizione, aderendo "alla piattaforma Web Analytics Italia (WAI), soluzione open source di raccolta, analisi e condivisione dei dati di traffico e comportamento utente dedicata ai siti web delle amministrazioni pubbliche italiane" (paragrafo 5.4 - "Monitoraggio dei servizi");

prevedere un'esperienza d'uso comune, garantendo specialmente l'accesso ai servizi digitali della pubblica amministrazione con i sistemi di autenticazione previsti dal CAD e consentire agli utenti di effettuare i pagamenti online con i sistemi di pagamento previsti dal medesimo codice (paragrafo 5.6 - "Integrazione delle piattaforme abilitanti").

OSSERVA

Preliminarmente, si osserva che lo schema in esame rappresenta un'opportunità per offrire ai titolari del trattamento, e ai soggetti a vario titolo coinvolti, indicazioni utili ad assicurare la protezione dei dati personali trattati dalle pubbliche amministrazioni nell'ambito della gestione dei siti web e dei servizi digitali, in ossequio al principio di privacy by design e by default (art. 25 del Regolamento).

Muovendo da tali considerazioni, si rileva la necessità che lo schema in esame sia opportunamente integrato, come di seguito indicato, affinché i trattamenti di dati personali posti in essere dai destinatari delle linee guida siano pienamente conformi ai richiamati principi e garanzie.

1. La sicurezza del trattamento

Con riguardo all'indicazione, contenuta nel paragrafo 5.2, di "garantire la protezione dei dati personali, nello sviluppo di un sito web o di un servizio digitale, fin dalla progettazione e per impostazione predefinita, nel rispetto dell'art. 25 del GDPR", si ritiene che sia integrata con un espresso rimando alle indicazioni fornite dal Comitato europeo per la protezione dei dati nelle "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita" adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020.

Lo schema di linee guida fa riferimento, inoltre, alla necessità di "rispettare almeno il livello base di sicurezza stabilito dalle «Misure minime di sicurezza ICT per le pubbliche amministrazioni», ove non sia specificamente richiesto un livello superiore dal citato documento". Premesso che la richiamata circolare dell'AgID del 18 aprile 2017, n. 2, è stata emanata prima della data di efficacia del Regolamento, si osserva, in via generale, che il rinvio alla stessa circolare, nell'ambito dei requisiti di sicurezza cui sono tenuti i vari soggetti coinvolti nel trattamento, non è di per sé sufficiente ad assicurare l'adozione di misure di sicurezza del trattamento "adeguate", in conformità al Regolamento, a norma del quale, occorre invece valutare, in concreto, i rischi che possono derivare, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati (cfr. parere del Garante sullo schema di "Linee guida - La Sicurezza nel procurement ICT" del 30 gennaio 2020, doc. web n. 9283857; parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" del 13 febbraio 2020, doc. web n. 9283921). Si evidenzia, pertanto, l'esigenza di riformulare il testo in commento, chiarendo che l'adozione delle predette misure minime non è di per sé idonea a soddisfare in tutti casi i requisiti previsti dagli artt. 5, par. 1, lett. f), e 32 del Regolamento, e che dunque una valutazione in tal senso deve essere effettuata, in maniera puntuale, dai titolari del trattamento.

Sotto altro profilo, si ravvisa la necessità di integrare lo schema precisando che, in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, il titolare, ai sensi dell'art. 35 del Regolamento, deve effettuare, prima di procedere al trattamento, una valutazione d'impatto sulla protezione dei dati, consultando preventivamente il Garante al ricorrere delle condizioni previste dall'art. 36 del Regolamento. A tal riguardo, lo schema potrebbe contenere un esplicito rimando alle indicazioni fornite dal Comitato europeo per la protezione dei dati nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679", WP 248 rev. 01, adottate dal Comitato europeo per la protezione dei dati il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017.

2. La trasparenza nei confronti degli interessati

Per quanto concerne, in generale, la necessità di assicurare la trasparenza dei trattamenti effettuati nei confronti degli interessati, si rileva che, come chiarito a livello europeo (v. le "Linee guida sulla trasparenza ai sensi del regolamento 2016/679", adottate dal 2Gruppo di lavoro articolo 29", il 29 novembre 2017 e modificate l'11 aprile 2018, WP260 rev.01, fatte proprie dal Comitato europeo per la protezione dei dati con "Endorsement 1/2018" del 25 maggio 2018), nello schema occorre specificare che:

- nel rispetto di quanto previsto dall'art. 12 del Regolamento, le informazioni sul trattamento

dei dati personali fornite agli utenti devono essere concise, trasparenti, intelligibili e facilmente accessibili, nonché formulate con un linguaggio semplice e chiaro, specialmente nel caso d'informazioni destinate ai minori;

su ogni pagina del sito dovrebbe essere chiaramente visibile un link diretto all'informativa sul trattamento dei dati personali, che riporti una dicitura di uso comune (come "Privacy", "Informativa sulla privacy" o "Informativa sulla protezione dei dati");

al momento della raccolta dei dati personali in ambiente online, deve, inoltre, essere fornito il link all'informativa sul trattamento dei dati personali o, in alternativa, le informazioni sul trattamento dei dati devono essere messe a disposizione sulla stessa pagina in cui sono raccolti i dati personali;

allorquando i siti web o i servizi digitali siano specificamente indirizzati a soggetti con disabilità, è necessario fare in modo che gli interessati possano effettivamente fruire dei contenuti dell'informativa sul trattamento dei dati personali;

nei casi in cui i siti web o i servizi digitali siano specificamente indirizzati, invece, ai minori, l'informativa da rendere agli interessati deve essere predisposta utilizzando un linguaggio semplice e chiaro, in modo che un minore possa comprendere facilmente i relativi contenuti.

Analogamente, qualora l'erogazione di servizi digitali avvenga mediante applicazioni per dispositivi mobili (app), le informazioni necessarie devono essere messe a disposizione presso gli store delle app prima del download. Una volta installata l'app, le informazioni devono continuare a essere facilmente accessibili al suo interno. Un modo per soddisfare questo requisito consiste nel garantire che le informazioni non siano mai a più di due "tocchi" di distanza (ad es. includendo un'opzione "Privacy"/"Protezione dei dati" nella funzione di menù dell'app). Inoltre, l'informativa sul trattamento dei dati personali deve riguardare specificamente l'app e non meramente l'informativa generica della pubblica amministrazione che è proprietaria dell'app o che la mette a disposizione pubblicamente (v. le "Linee guida sulla trasparenza ai sensi del regolamento 2016/679", cit.).

Si ravvisa, infine, l'esigenza che lo schema di linee guida in esame evidenzi alle pubbliche amministrazioni l'obbligo, previsto dall'art. 37, par. 7, del Regolamento, di pubblicare i dati di contatto del responsabile della protezione dei dati (RPD), che le stesse sono tenute a designare ai sensi dell'art. 37, par. 1, lett. a), del Regolamento. Come indicato nel "Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico" (doc. web n. 9589467) allegato al provv. 29 aprile 2021, n. 186 (doc. web n. 9589104), la pubblicazione di tali dati di contatto deve essere effettuata sul sito web dell'amministrazione, all'interno di una sezione facilmente riconoscibile dall'utente e accessibile già dalla homepage, oltre che nell'ambito della sezione dedicata all'organigramma dell'ente e ai relativi contatti. Non è necessario che, tra i dati oggetto di pubblicazione, vi sia anche il nominativo del RPD, non essendo questa informazione indispensabile a fini di contatto da parte di chiunque sia interessato: al contrario, risulta imprescindibile che tra i dati di contatto vi sia quantomeno un indirizzo di posta elettronica ordinaria (e, eventualmente, un indirizzo di posta elettronica certificata).

3. L'utilizzo di cookie o di altri strumenti di tracciamento

Occorre evidenziare, nelle linee guida in esame, che l'utilizzo di cookie o altri strumenti di tracciamento nell'ambito di un sito web o un servizio digitale richiede un'attenta valutazione in ordine alla necessità del ricorso agli stessi rispetto alle finalità perseguite dalla pubblica amministrazione. Tale valutazione deve riguardare, altresì, la base giuridica degli eventuali successivi trattamenti che si intendono porre in essere attraverso i dati personali raccolti dai dispositivi degli utenti sulla base dell'art. 122 del Codice, tenendo conto anche delle garanzie da assicurare in relazione a possibili trasferimenti di dati verso Paesi terzi che, in ogni caso, devono

avvenire nel rispetto degli artt. 44 e ss. del Regolamento.

Innanzitutto, con riguardo al rispetto del principio di trasparenza e alla necessità, prospettata nello schema in esame, di "pubblicare, sul singolo sito, l'informativa sul trattamento dei dati personali" (paragrafo 5.2), si evidenzia che, allorquando nel sito web e nel servizio digitale siano utilizzati dei c.d. cookie o altri strumenti di tracciamento, i titolari del trattamento, ai sensi degli artt. 12 e 13 del Regolamento, nonché 122 del Codice, devono informare gli utenti in merito all'impiego degli stessi, con le modalità illustrate nelle "Linee guida cookie e altri strumenti di tracciamento" del 10 giugno 2021 (doc. web n. 9677876), che integrano e precisano quanto illustrato nel precedente provvedimento del Garante "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie" dell'8 maggio 2014, n. 229 (doc. web n. 3118884).

Con specifico riferimento all'individuazione delle fattispecie in cui è necessario acquisire un consenso all'utilizzo di cookie o di altri strumenti di tracciamento e alle modalità di acquisizione dello stesso, che devono avvenire nel rigoroso rispetto del principio di correttezza, si evidenzia la necessità di richiamare espressamente le citate "Linee guida cookie e altri strumenti di tracciamento", assicurando, in ogni caso, la piena fruibilità del sito web o del servizio digitale anche laddove l'utente non intenda prestare il proprio consenso all'archiviazione di informazioni sul proprio dispositivo o all'accesso alle informazioni ivi archiviate.

Con riguardo all'invito ad "aderire alla piattaforma Web Analytics Italia (WAI), soluzione open source di raccolta, analisi e condivisione dei dati di traffico e comportamento utente dedicata ai siti web delle amministrazioni pubbliche italiane", nel rappresentare che tale piattaforma non è stata sottoposta all'attenzione del Garante, che si riserva di effettuare gli opportuni approfondimenti al riguardo, si evidenzia la necessità che gli utenti ne siano debitamente informati ai sensi degli artt. 12 e 13 del Regolamento e 122 del Codice, assicurando il rispetto di quanto previsto nelle richiamate linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento. Occorre, altresì, richiamare l'attenzione sulla necessità di definire e disciplinare i ruoli e le responsabilità del fornitore di tale piattaforma ai fini del rispetto della normativa in materia di protezione dei dati.

4. Rapporti con i fornitori dei servizi

Con riguardo all'indicazione di "nominare Responsabili del trattamento ai sensi dell'art. 28 del GDPR gli eventuali fornitori dei servizi web che trattano dati personali per conto del soggetto titolare del trattamento", si evidenzia la necessità di specificare che il titolare deve:

ricorrere "unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato", anche in considerazione dei rischi per i diritti e le libertà degli interessati e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento effettuato, derivanti anche da eventuali trasferimenti di dati verso Paesi terzi;

regolare i trattamenti svolti per suo conto da parte del responsabile attraverso un accordo sulla protezione dei dati, individuando adeguatamente l'ambito e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento e, inoltre, vengano documentate le istruzioni fornite al responsabile del trattamento (art. 28 del Regolamento);

disciplinare la possibilità per il responsabile del trattamento di ricorrere ad altro responsabile, in conformità all'art. 28, parr. 2 e 4, del Regolamento, individuando misure organizzative volte a garantire al titolare del trattamento, in ossequio al principio di accountability, idonei strumenti di controllo delle attività di trattamento effettuate sotto la propria responsabilità (ad

esempio, modalità di aggiornamento dell'elenco degli altri responsabili);

individuare una corretta ripartizione delle responsabilità tra titolare e responsabile per quanto concerne il trattamento dei dati personali effettuato nell'ambito dei siti web e dei servizi digitali, anche in relazione all'adozione di adeguate misure tecniche e organizzative, evitando, in particolare, sproporzionati esoneri di responsabilità, soprattutto in caso di contratti standard, con margini di negoziazione pressoché nulli in capo al titolare del trattamento.

Ciò non solo nei rapporti con i "fornitori dei servizi web", bensì con qualunque fornitore di servizi informatici, come, ad esempio, i fornitori di servizi di hosting o cloud computing, rispetto ai quali l'amministrazione agisce in qualità di titolare (sul punto, v. le "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, in particolare punti 30 e 40). Il documento in esame dovrebbe, inoltre, evidenziare che, allorquando tali fornitori di servizi siano stabiliti in Paesi terzi, occorre, altresì, soddisfare le condizioni previste dagli artt. 44 e ss. del Regolamento ai fini della liceità del trasferimento dei dati personali in tali Paesi.

5. L'utilizzo dei sistemi di autenticazione e di elementi di terze parti

Lo schema di linee guida in esame, nel ricordare che "si deve garantire l'accesso ai servizi digitali della PA con i sistemi di autenticazione previsti dal CAD" (paragrafo 5.6), deve evidenziare che, nel progettare i servizi digitali, occorre garantire il rispetto del principio di minimizzazione di dati, assicurando che, nell'ambito delle procedure di autenticazione informatica, siano acquisiti e successivamente trattati solo dati personali degli utenti (attributi dell'identità digitale) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, par. 1, lett. c), del Regolamento e art. 27 del Regolamento recante le modalità attuative per la realizzazione dello SPID).

Si ritiene necessario, infine, esplicitare nello schema che l'utilizzo di eventuali elementi di terze parti incorporati sui propri siti web (ad esempio, font tipografici, video player, social plug-in, ecc.) può comportare la comunicazione di dati personali a terzi, nonché, in taluni casi, anche il trasferimento dei dati personali in Paesi terzi, che richiedono valutazioni, caso per caso, in ordine alla sussistenza di un'idonea base giuridica (cfr. artt. 5, par. 1, lett. a), e 6 del Regolamento, nonché 2-ter del Codice) e di adeguate garanzie ai sensi degli artt. 44 e ss. del Regolamento.

RITENUTO

Alla luce di quanto sopra osservato, si ritiene necessario che lo schema di Linee guida in esame venga integrato con gli elementi indicati nei paragrafi da 1 a 5, al fine di fornire alle amministrazioni pubbliche destinatarie di tali Linee guida, le indicazioni corrette per assicurare la conformità al Regolamento e al Codice dei trattamenti dei dati personali effettuati nell'ambito della progettazione e gestione dei siti web e dei servizi digitali.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi degli artt. 36, par. 4, e 58, par. 3, lett. b), del Regolamento, esprime parere favorevole sullo schema di "Linee guida di design per i siti internet e i servizi digitali della PA", predisposto da AgID, ai sensi degli artt. 53, comma 1-ter, e 71 del d.lgs. 7 marzo 2005, n. 82, a condizione che sia integrato con le indicazioni relative a:

la sicurezza del trattamento (par. 1);

la trasparenza nei confronti degli interessati (par. 2);

l’utilizzo di cookie o di altri strumenti di tracciamento (par. 3);

i rapporti con i fornitori dei servizi (par. 4);

l’utilizzo dei sistemi di autenticazione e di elementi di terze parti (par. 5).

Roma, 24 febbraio 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei