GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 2574977]

Linee guida redatte dall'Agenzia per l'Italia Digitale ai sensi dell'art. 58, comma 2, del d.lg. 7 marzo 2005, n. 82 (CAD) - 4 luglio 2013

Registro dei provvedimenti
n. 332 del 4 luglio 2013

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, della e del dott. Giuseppe Busia, segretario generale;

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

VISTA la richiesta di parere dell'Agenzia per l'Italia digitale del 6 giugno 2013 sulle linee guida redatte ai sensi dell'art. 58, comma 2, del d.lg. 7 marzo 2005, n. 82;

VISTA la documentazioni 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

L'Agenzia per l'Italia Digitale, con la nota del 6 giugno 2013, ha sottoposto al Garante le linee guida redatte ai sensi dell'art. 58, comma 2, del d.lg. 7 marzo 2005, n. 82 (di seguito Cad). Tale disposizione prevede, infatti, che, *"ai sensi dell'articolo 50, comma 2, nonché al fine di agevolare l'acquisizione d'ufficio ed il controllo sulle dichiarazioni sostitutive riguardanti informazioni e dati relativi a stati, qualità personali e fatti di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le Amministrazioni titolari di banche dati accessibili per via telematica predispongono apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico. Le convenzioni valgono anche quale autorizzazione ai sensi dell'articolo 43, comma 2, del citato decreto del Presidente della Repubblica n. 445 del 2000"*.

Nell'aprile 2011, DigitPA, ora Agenzia per l'Italia Digitale, aveva pubblicato una prima versione delle predette linee guida in relazione alla quale, in collaborazione con l'Ufficio del Garante, sono state apportate modifiche e integrazioni volte, in particolare, a migliorare gli aspetti relativi alle convenzioni che hanno per oggetto l'accesso a dati personali, ora riportate nella versione in esame. Tale nuova versione delle linee guida tiene anche conto delle recenti modifiche normative che, in particolare, hanno istituito l'Agenzia e ne hanno definito le competenze (d.l. 22 giugno 2012, n. 83, convertito con modificazioni con la legge n. 134/2012) e sono intervenute in materia di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni (d.lg. 14 marzo 2013, n. 33).

In particolare, le linee guida individuano:

a. i destinatari e il contesto, anche normativo, di riferimento (par. 3);

b. le modalità di raccolta e formazione dei dati, anche con riferimento ai fini statistici, in relazione a quanto previsto dalla normativa vigente in materia (par. 4);

c. i servizi e le modalità che dovranno essere utilizzate per l'accesso ai dati delle pubbliche amministrazioni, con l'indicazione dei criteri per la definizione dei livelli di servizio che le convenzioni potranno stabilire. In tale contesto, viene data particolare attenzione ai casi in cui la convenzione abbia per oggetto l'accesso a dati personali (par. 5);

d. la struttura della convenzione-quadro, con l'indicazione del contenuto minimo della stessa e degli aspetti che devono essere disciplinati (par. 6);

e. il procedimento e gli adempimenti connessi alla stipula della convenzione, anche ai fini delle attività di monitoraggio poste in capo all'Agenzia per l'Italia Digitale (par. 7).

A completamento delle linee guida viene riportato, in allegato alle stesse, un estratto della normativa di riferimento (all. 1), nonché i "Criteri tecnici per le modalità di accesso" da prevedere nelle convenzioni, che descrivono gli aspetti tecnici e di sicurezza delle differenti modalità di accesso previste (all. 2).

Le linee guida verranno adottate con determinazione del Direttore Generale dell'Agenzia per l'Italia digitale e saranno pubblicate sul sito istituzionale dell'Agenzia per l'Italia Digitale.

Viene, inoltre, previsto che l'aggiornamento delle linee guida potrà avvenire con le stesse modalità, sentito il Garante, in relazione all'evoluzione delle tecnologie ed all'esigenza di introdurre ulteriori misure a garanzia della sicurezza dei dati e del loro corretto trattamento.

OSSERVA:

Il parere è reso su di una versione delle linee guida che tiene conto degli approfondimenti e delle indicazioni suggeriti dall'Ufficio del Garante ai competenti uffici dell'Agenzia nel corso di riunioni e contatti informali, volti a perfezionare il testo e a rendere conformi alla disciplina in materia di protezione dei dati personali i trattamenti ivi previsti.

Le osservazioni dell'Ufficio hanno interessato principalmente il paragrafo 5 delle linee guida "Servizi e modalità di accesso alle banche dati", con particolare riferimento al sotto paragrafo 5.5. dedicato agli "Aspetti di protezione dei dati personali", nonché i paragrafi 6 e 7 relativi, rispettivamente, al "Contenuto della convenzione" e agli "Adempimenti di attuazione" che sono state integralmente recepite dall'Agenzia. Pertanto, il Garante esprime parere favorevole sulle linee guida in esame.

In particolare, il testo così modificato, oltre a prevedere il necessario rispetto delle misure minime previste dal Codice (art. 33), reca anche le misure necessarie che il Garante, ai sensi dell'articolo 154, comma 1, lett. c), del Codice, ritiene di prescrivere ai destinatari delle linee guida ("erogatore" e "fruitore" dei dati) al fine di ridurre al minimo i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento (art. 31 del Codice).

Di conseguenza, nell'Allegato 1 al presente provvedimento, che ne costituisce parte integrante, vengono individuate le misure necessarie, contenute nei corrispondenti paragrafi delle linee guida, che l'erogatore e il fruitore dei dati sono tenuti a rispettare nel trattamento dei dati personali oggetto delle convenzioni stipulate ai sensi dell'art. 58 del Cad. In caso di inosservanza delle predette misure da parte degli stessi sarà applicata la sanzione amministrativa di cui all'art. 162, comma 2-ter, del Codice.

Laddove siano già state stipulate convenzioni ai sensi del predetto art. 58, comma 2, del Cad prima dell'adozione delle linee guida in esame da parte dell'Agenzia per l'Italia Digitale, le misure necessarie individuate nel presente provvedimento dovranno essere rispettate in occasione del rinnovo delle convenzioni stesse e, comunque, entro e non oltre il 30 giugno 2014.

Restano salve le convenzioni o le modalità di accesso alle banche dati che siano già state oggetto di esame da parte del Garante per la protezione dei dati personali nell'ambito di specifici provvedimenti.

Si ritiene, inoltre, necessario che l'Agenzia per l'Italia Digitale:

- garantisca la massima conoscibilità delle misure necessarie prescritte dal Garante nel presente provvedimento ai destinatari delle linee guida evidenziandole opportunamente nel testo, facendo anche riferimento alle conseguenze in caso di inosservanza, consistenti nell'applicazione, da parte del Garante, della sanzione amministrativa di cui all'art. 162, comma 2-ter, del Codice;

- segnali al Garante le difformità relative agli aspetti di sicurezza e protezione dei dati personali rilevate nell'ambito dei controlli effettuati dall'Agenzia stessa sulle convenzioni-quadro ai sensi del punto 4 del paragrafo 7 delle linee guida;

- metta a disposizione del Garante per via telematica, entro il 31 ottobre 2013, un documento aggiornato contenente i dati relativi alle convenzioni individuati nello schema riportato al punto 6 del paragrafo 7 delle linee guida, anche in relazione ai casi in cui la fruizione dei dati avvenga in modalità di cooperazione applicativa. Ciò, al fine di agevolare le procedure di controllo dell'Autorità, anche in coordinamento con la medesima Agenzia.

TUTTO CIO' PREMESSO IL GARANTE:

I. ai sensi dell'articolo 154, commi 1, lett. g), e 5, del Codice, esprime parere favorevole sulle linee guida in esame redatte dall'Agenzia per l'Italia Digitale ai sensi dell'art. 58, comma 2, del d.lg. 7 marzo 2005, n. 82;

II. ai sensi dell'articolo 154, comma 1, lett. c), del Codice, al fine di ridurre al minimo i rischi di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalità della raccolta dei dati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento nell'ambito delle convenzioni stipulate ai sensi dell'art. 58, comma 2 del Cad, prescrive ai destinatari delle predette linee guida di adottare le misure necessarie individuate nell'Allegato 1 al presente provvedimento, salvo che le convenzioni medesime o le modalità di accesso alle banche dati siano già state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti. Laddove siano già state stipulate convenzioni ai sensi del predetto art. 58, comma 2 del Cad, prima dell'adozione delle linee guida in esame da parte dell'Agenzia per l'Italia Digitale, le misure necessarie individuate nel presente provvedimento dovranno essere rispettate in occasione del rinnovo delle stesse convenzioni e, comunque, entro e non oltre il 30 giugno 2014;

III. ai sensi dell'articolo 154, comma 1, lett. c), del Codice, prescrive all'Agenzia per l'Italia Digitale di:

1) garantire la massima conoscibilità delle misure necessarie prescritte dal Garante nel presente provvedimento ai destinatari delle linee guida evidenziandole opportunamente nel testo, anche facendo riferimento alle conseguenze in caso di inosservanza delle stesse, consistenti nell'applicazione, da parte del Garante, della sanzione amministrativa di cui all'art. 162,

comma 2-ter, del Codice;

2) segnalare al Garante le difformità relative agli aspetti di sicurezza e protezione dei dati personali rilevate nell'ambito dei controlli effettuati dall'Agenzia sulle convenzioni-quadro ai sensi del punto 4 del paragrafo 7 delle linee guida;

3) mettere a disposizione del Garante per via telematica, entro il 31 ottobre 2013, un documento aggiornato contenente i dati relativi alle convenzioni individuati nello schema riportato al punto 6 del paragrafo 7 delle linee guida, anche in relazione ai casi in cui la fruizione dei dati avvenga in modalità di cooperazione applicativa.

Roma, 4 luglio 2013

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia

Allegato 1

Misure necessarie

5.1 Modalità d'accesso

…... "le pubbliche amministrazioni devono rendere conoscibili le diverse tipologie di dati che possono essere fruibili da altre pubbliche amministrazioni, mediante pubblicazione sul proprio sito istituzionale delle convenzioni-quadro volte a disciplinare le modalità di accesso ai dati.

In proposito, tenuto conto degli obiettivi di carattere generale perseguiti dal CAD e dell'attuale quadro infrastrutturale disponibile sul territorio, si prevedono le seguenti opzioni tecniche per la fruibilità dei dati:

- accesso via web, attraverso il sito istituzionale dell'erogatore o un sito tematico all'uopo predisposto;

- accesso in modalità di cooperazione applicativa, componente del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi."….

5.2 Modalità d'accesso alternative e transitorie

"Fermo restando le modalità di accesso telematico definite al punto precedente, che devono considerarsi quelle di riferimento ai fini dell'attuazione delle norme in materia di fruibilità dei dati, le amministrazioni possono utilizzare modalità alternative, laddove si presentino documentabili vantaggi economici o la situazione infrastrutturale e organizzativa non consenta l'adozione di quelle sopra riportate. Le predette circostanze devono essere adeguatamente documentate all'Agenzia per l'Italia Digitale e richiamate in convenzione. In tali casi, le modalità di accesso telematico prevedibili sono:

- la posta elettronica certificata, nei casi specifici, quando la periodicità di acquisizione del dato è limitata (in linea di massima una volta all'anno o meno) e la quantità dei dati da acquisire è contenuta;

- soluzioni di "Trasferimento di File" in modalità FTP "sicuro" o equivalente dal punto di vista della sicurezza del trasporto, qualora preesistenti investimenti, la natura stessa delle richieste e le specifiche condizioni facciano propendere per tale soluzione garantendo la cifratura del canale di trasmissione dei dati (ad esempio, utilizzando meccanismi quali le reti private virtuali)."….

5.5 Aspetti di protezione dei dati personali

Qualora la convenzione abbia per oggetto l'accesso a dati personali, nel trattamento di tali informazioni l'erogatore e il fruitore sono chiamati a rispettare le disposizioni del Codice con particolare riferimento ai presupposti che legittimano i flussi di dati e agli adempimenti in materia di misure di sicurezza.

Le convenzioni sono lo strumento in cui stabilire le garanzie poste - anche nei confronti dello stesso erogatore - a tutela del trattamento dei dati personali e dell'utilizzo dei sistemi informativi.

Di seguito vengono pertanto individuati misure e accorgimenti da attuare al fine di assicurare la correttezza del trattamento e di ridurre rischi nell'utilizzo dei dati personali.

In ogni caso l'erogatore, al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle

banche dati accessibili attraverso la convenzione, è tenuto a valutare l'introduzione di ulteriori strumenti volti a gestire i profili di autorizzazione, verificare accessi anomali, tracciare le operazioni di accesso, ovvero individuare tassative modalità di accesso alle banche dati, dandone conto nella convenzione (art. 31 del Codice).

5.5.1 Presupposti per l'accesso alle banche dati

5.5.1.1 Verifiche preliminari

L'erogatore prima di stipulare ogni singola convenzione per l'accesso alle proprie banche dati in via telematica deve verificare:

a) la base normativa che legittima il fruitore ad accedere alle proprie banche dati (norma di legge o di regolamento, anche ai sensi dell'art. 19, comma 2 del Codice, previa comunicazione al Garante), specie in caso di dati sensibili e giudiziari (cfr. paragrafo 5.5.3.);

b) la finalità istituzionale perseguita dal fruitore (ad esempio controllo sulle dichiarazioni sostitutive) e la natura e la qualità dei dati richiesti, selezionando accuratamente le informazioni personali contenute nelle banche dati a cui dare accesso;

c) la modalità telematica di accesso alle banche dati più idonea rispetto alle finalità, alla natura e alla quantità dei dati, alle caratteristiche anche infrastrutturali e organizzative del fruitore, al volume e alla frequenza dei trasferimenti, il numero di soggetti abilitati all'accesso.

5.5.1.2 Selezione dei dati

La selezione delle informazioni personali oggetto di accesso deve avvenire nel rispetto dei principi di pertinenza e non eccedenza in relazione a ciascuna delle finalità perseguite dal fruitore. Rispetto ad una medesima banca dati devono essere, infatti, prefigurati diversi livelli e modalità di accesso che offrano al fruitore unicamente i dati necessari per le proprie esigenze istituzionali.

Le modalità di accesso alle banche dati devono essere, pertanto, configurate offrendo un livello minimo di accesso ai dati, anche limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., web services che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un dato oggetto di autocertificazione). Livelli di accesso gradualmente più ampi possono essere autorizzati soltanto a fronte di documentate esigenze del fruitore da indicare in convenzione.

È chiaro, inoltre, che per ciascun fruitore possono essere individuate più modalità di accesso ad una medesima banca dati in relazione alle diverse funzioni svolte dai propri operatori per il perseguimento della medesima finalità, modulando così il livello di accesso ai dati. L'erogatore deve, infatti, far sì che sia consentita, per quanto più possibile, la segmentazione dei dati visualizzabili al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza del fruitore, esclusivamente i dati necessari rispetto alle finalità in concreto perseguite. In altri termini la convenzione deve prevedere l'accesso alle sole informazioni pertinenti e non eccedenti rispetto alla finalità istituzionale perseguita dalla convenzione stessa.

Particolare attenzione deve essere prestata, inoltre, nella scelta delle informazioni richieste per l'interrogazione diretta della banca dati, ovvero per l'invocazione dei web services, imponendo un set minimo di dati per l'individuazione puntuale del soggetto cui si riferiscono. Salvo eccezioni rigorosamente motivate e documentate nella convenzione, la risposta fornita all'interrogazione non deve, poi, contenere un elenco di soggetti.

5.5.1.3 Elenco aggiornato

L'erogatore deve poi disporre in ogni momento di informazioni complete e strutturate sui fruitori autorizzati e sulle modalità di accesso alle proprie banche dati.

A tal fine occorre pertanto che l'erogatore rediga un documento, mantenuto costantemente aggiornato, che riporti l'elenco delle banche dati accessibili, descrivendo per ogni fruitore le informazioni di cui ai punti a), b), c), di cui al precedente paragrafo 5.5.1.1, corredato delle informazioni relative ai formati dei dati disponibili a fruitori esterni ("tracciato record", schemi XML o altri formalismi).

5.5.1.4 Controlli annuali

L'erogatore deve altresì verificare, con cadenza periodica annuale, l'attualità delle finalità per cui ha concesso l'accesso ai fruitori, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) non conformi a quanto stabilito nelle convenzioni.

5.5.2 Soggetti incaricati del trattamento

5.5.2.1 Designazione responsabili e incaricati

Per effetto dell'esecuzione della convenzione e della conseguente comunicazione dei dati personali, il fruitore, in quanto titolare del trattamento dei dati oggetto di comunicazione da parte dell'erogatore, ai sensi della normativa vigente in materia, deve dare attuazione a quanto previsto dagli artt. 29 e 30 del Codice della privacy, in materia di designazione degli incaricati del trattamento e eventuale designazione del responsabile del trattamento, garantendo che l'accesso ai dati sia consentito esclusivamente a tali soggetti.

Il fruitore si impegna a comunicare all'erogatore, su richiesta motivata, l'elenco degli incaricati del trattamento autorizzati all'accesso ai dati (ad esempio, in caso di controlli sull'attualità delle utenze la cui amministrazione è demandata a gestori presso il fruitore, ovvero nel caso di

cooperazione applicativa di cui al punto seguente).

Laddove i fruitori vogliano avvalersi di soggetti terzi (ad esempio, altra pubblica amministrazione o altro soggetto) al fine di realizzare servizi d'interscambio, previa apposita designazione dello stesso soggetto delegato come responsabile o, se persona fisica, anche incaricato del trattamento dei dati personali, devono darne comunicazione all'erogatore. Tale eventualità deve essere, naturalmente, esplicitamente riportata nella convenzione.

5.5.2.2 Procedura di autenticazione e autorizzazione degli utenti

a) Accessi via web

Nel caso in cui la modalità di accesso prescelta preveda l'attribuzione di credenziali individuali (ad esempio, applicazione con accesso via web), le convenzioni devono predefinire una procedura per il rilascio delle utenze e la gestione delle autorizzazioni degli utenti che coinvolga attivamente le figure apicali degli uffici interessati e un unico supervisore (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con il soggetto tecnicamente deputato alla materiale gestione delle utenze (direttamente o attraverso l'erogatore), ma deve rispondere del controllo sullo stesso.

Nel caso il sistema di accesso preveda la gestione diretta delle utenze da parte del fruitore, la convenzione deve prevedere l'individuazione di uno o più soggetti (coordinati tra loro) deputati alla materiale amministrazione delle utenze di coloro che sono stati autorizzati dal supervisore ad accedere alla banca dati. Tali gestori-amministratori devono essere preferibilmente scelti tra personale che abbia un rapporto stabile con il fruitore e devono essere adeguatamente formati in ordine alle modalità di accesso alla banca dati e all'attività di autorizzazione degli utenti.

Occorre inoltre che venga assicurato un flusso di comunicazione tra il supervisore, il gestore e l'articolazione che si occupa della gestione delle risorse umane, al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente, anche con apposite verifiche a cadenza almeno trimestrale. Il responsabile della convenzione individuato presso il fruitore deve effettuare periodicamente, con cadenza almeno annuale, anche in collaborazione con l'erogatore, una puntuale verifica sulla corretta attribuzione dei profili di autorizzazione e sull'attualità delle utenze attive. Le convenzioni devono predefinire anche le soglie relative al numero di utenti abilitabili da ciascun fruitore.

L'elenco dei soggetti incaricati da abilitare all'accesso alla banca dati deve essere allegato alla convenzione, ovvero comunicato entro un termine ivi stabilito, e costantemente aggiornato dal responsabile della convenzione. Qualora la gestione degli utenti sia demandata al fruitore, la comunicazione potrà essere limitata agli utenti cui è affidata la funzione di gestori dell'amministrazione delle utenze.

b) Cooperazione applicativa

I web services devono essere integrati soltanto in applicativi che gestiscono procedure amministrative volte al raggiungimento delle finalità istituzionali per le quali è consentita la comunicazione delle informazioni contenute nella banca dati. Devono essere, quindi, possibili unicamente accessi per le finalità per le quali è stata realizzata la convenzione alle sole informazioni pertinenti e non eccedenti rispetto alla finalità istituzionale perseguita dalla convenzione.

In ogni caso, il fruitore deve garantire che i servizi resi disponibili dall'erogatore verranno esclusivamente integrati con il proprio sistema informativo e tali servizi non saranno resi disponibili a terzi per via informatica.

Le modalità di accesso in cooperazione applicativa integrata negli applicativi utilizzati dal fruitore devono assicurare garanzie non inferiori a quelle individuate nel precedente punto a) attraverso idonee policy di sicurezza dei sistemi informativi dello stesso, che prevedano la presenza di una figura apicale (anche coadiuvata da un responsabile tecnico) a garanzia del rispetto dei presupposti per l'accesso stabiliti in convenzione, anche attraverso verifiche periodiche, in termini di:

- gestione delle utenze;

- profili di autorizzazione degli utenti in relazione ai dati ottenuti dall'erogatore mediante la piattaforma del fruitore;

- misure di sicurezza.

Al fine di consentire l'adeguato tracciamento delle operazioni compiute sui dati personali, il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione; il suddetto codice identificativo, anche nel caso in cui l'accesso avvenga attraverso sistemi di cooperazione applicativa, deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione; il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilità, su richiesta, di identificare l'utente nei casi in cui ciò si renda necessario.

5.5.2.3 Istruzioni e correttezza del trattamento

Il fruitore deve utilizzare le informazioni acquisite esclusivamente per le finalità dichiarate in convenzione, nel rispetto dei principi di pertinenza e non eccedenza, nonché di indispensabilità, per i dati sensibili e giudiziari.

Il fruitore deve, altresì, garantire che non si verifichino divulgazioni, comunicazioni, cessioni a terzi, né in alcun modo riproduzioni dei dati nei casi diversi da quelli previsti dalla legge, stabilendo le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche

attraverso l'utilizzo di strumenti automatizzati di interrogazione. A tal fine il fruitore si impegna ad utilizzare i sistemi di accesso ai dati in consultazione on line esclusivamente secondo le modalità con cui sono stati resi disponibili e, di conseguenza, a non estrarre i dati per via automatica e massiva (attraverso ad esempio i cosiddetti "robot") allo scopo, ad esempio, di velocizzare le attività e creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato all'accesso;

Il fruitore deve garantire, inoltre, che l'accesso ai dati verrà consentito esclusivamente a personale o assimilati ovvero a soggetti che siano stati designati dal fruitore quali incaricati o responsabili del trattamento dei dati, impartendo, ai sensi degli artt. 29 e 30 del Codice, precise e dettagliate istruzioni, richiamando la loro attenzione sulle responsabilità connesse all'uso illegittimo dei dati, nonché al corretto utilizzo delle funzionalità dei collegamenti.

5.5.3 Dati sensibili e giudiziari

In ogni caso, qualora sia indispensabile accedere a dati sensibili o giudiziari, questi devono essere opportunamente cifrati con algoritmi che garantiscano livelli di sicurezza adeguati al contesto ai sensi dell'art. 22, comma 6, del Codice.
In considerazione della delicatezza e della quantità di informazioni scambiate, l'erogatore deve individuare le modalità di trasferimento dei dati sensibili e giudiziari maggiormente idonee ad assicurare la sicurezza dei collegamenti, prevedendo che in ogni caso il trasferimento dei dati idonei a rivelare lo stato di salute deve essere in ogni caso cifrato.

5.5.4 Misure di sicurezza

Oltre a garantire il rispetto delle misure minime di sicurezza previste dall'artt. 33 e ss. Codice e dal relativo Allegato B, al fine di adempiere agli obblighi di sicurezza di cui all'art. 31 del Codice nella fruibilità dei dati oggetto della convenzione (sia in caso di accessi via web che di cooperazione applicativa), l'erogatore e il fruitore devono assicurare che:

a. gli accessi alle banche dati avvengano soltanto tramite l'uso di postazioni di lavoro connesse alla rete Ip dell'ente autorizzato e/o dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti dell'erogatore, anche attraverso procedure di accreditamento che consentano di definire reti di accesso sicure (circuiti privati virtuali);

b. laddove l'accesso alla banca dati dell'erogatore avvenga in forma di web application esposta su rete pubblica (Internet), l'applicazione sia implementata con protocolli di sicurezza provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una Certification Authority ufficiale;

c. le procedure di registrazione avvengano con il riconoscimento diretto e l'identificazione certa dell'utente;

d. le regole di gestione delle credenziali di autenticazione prevedano, in ogni caso:

- l'identificazione univoca di una persona fisica;

- processi di emissione e distribuzione delle credenziali agli utenti in maniera sicura seguendo una procedura operativa prestabilita, o di accettazione di forme di autenticazione forte quali quelle che prevedono l'uso combinato di one time password o di certificati di autenticazione (CNS o analoghi);

- che le credenziali siano costituite da un dispositivo in possesso ed uso esclusivo dell'incaricato provvisto di pin o una coppia username/password, ovvero da credenziali che garantiscano analoghe condizioni di robustezza;
e. nel caso le credenziali siano costituite da una coppia username/password, siano adottate le seguenti politiche di gestione delle password:

- la password, comunicata direttamente al singolo incaricato separatamente rispetto al codice per l'identificazione (user id), sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi e le ultime tre password non possano essere riutilizzate;

- le password devono rispondere a requisiti di complessità (almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi);

- quando l'utente si allontana dal terminale, la sessione deve essere bloccata, anche attraverso eventuali meccanismi di time-out;

- le credenziali devono essere bloccate a fronte di reiterati tentativi falliti di autenticazione;

f. devono essere sempre presenti misure di protezione perimetrali logico-fisiche, quali ad esempio firewall e reti private virtuali (VPN);

g. i sistemi software, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui server che sulle postazioni di lavoro;

h. le misure di sicurezza devono periodicamente essere riconsiderate ed adeguate ai progressi tecnici e all'evoluzione dei rischi;

i. la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di

robustezza adeguata;

j. siano introdotti meccanismi volti a permettere il controllo degli accessi al fine di garantire che avvengano nell'ambito di intervalli temporali o di data predeterminati, eventualmente definiti sulla base delle esigenze d'ufficio;

k. in caso di accessi via web deve essere di regola esclusa la possibilità di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse;

l. entrambi si impegnano a comunicare tempestivamente:

- incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza afferenti la fruibilità di dati oggetto di convenzione;

- ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;

- ogni modificazione tecnica od organizzativa del proprio dominio, che comporti l'impossibilità di garantire l'applicazione delle regole di sopra riportate o la loro perdita di efficacia;

m. tutte le operazioni di trattamento di dati personali effettuate dagli utenti autorizzati, ivi comprese le utenze di tipo applicativo e sistemistico, devono essere adeguatamente tracciate. Al tal fine:

- il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione;

- il suddetto codice identificativo, anche nel caso in cui l'accesso avvenga attraverso sistemi di cooperazione applicativa, deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione;

- il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilità, su richiesta, di identificare l'utente nei casi in cui ciò si renda necessario.

5.5.5 Controlli

L'erogatore e il fruitore devono predisporre idonee procedure di audit sugli accessi alle banche dati, i cui esiti devono essere documentati secondo le modalità definite nelle convenzioni.

In particolare, devono essere introdotte attività di audit basate sul monitoraggio statistico delle transazioni e su meccanismi di alert che individuino comportamenti anomali o a rischio.

A tal fine, nelle applicazioni volte all'uso interattivo da parte di incaricati deve essere inserito un campo per l'indicazione obbligatoria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

Le suddette procedure devono, inoltre, prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso (quali, in particolare, la rispondenza delle interrogazioni ad una precisa finalità amministrativa).

5.5.6 Casi particolari

Come sopra ricordato, è compito dell'erogatore valutare l'introduzione di eventuali ulteriori misure e accorgimenti al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione (ad esempio, delicatezza e rilevanza delle informazioni accedute, rilevanti dimensioni della banca dati o del numero di utenti o volume di trasferimenti). Tali misure possono riguardare, in particolare:

- l'individuazione di tassative modalità di accesso alle banche dati;

- la gestione diretta da parte dell'erogatore dei profili di abilitazione, con la conoscenza dei dati identificativi dei soggetti autorizzati all'accesso alla banca dati per la realizzazione delle finalità istituzionali dichiarate nella convenzione;

- l'utilizzo di strumenti di strong authentication per l'autenticazione informatica di particolari categorie di utenti;

- in caso di accessi via web:

  - nella prima schermata successiva al collegamento con la banca dati, siano visualizzabili le informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione);

- le informazioni di cui al punto precedente devono essere riportate anche relativamente alla sessione corrente;

- la verifica di accessi anomali attraverso strumenti di business intelligence per monitorare gli accessi attraverso i log relativi a tutti gli attuali e futuri applicativi utilizzati da parte dei fruitori, ovvero attraverso specifiche procedure di audit dell'erogatore presso il fruitore.

7. Adempimenti di attuazione

Le amministrazioni titolari di banche dati accessibili per via telematica predispongono sulla base delle presenti linee guida convenzioni-quadro aperte all'adesione delle amministrazioni interessate.

In relazione a tale adempimento procedurale possono prevedersi, in linea generale, i seguenti casi:

a) la convenzione ha per oggetto l'accesso a dati personali, secondo quanto previsto dall'articolo 4, lett. b), del D. Lgs. 30 giugno 2003, n. 196; in questo caso, l'adempimento in parola può ritenersi soddisfatto esclusivamente a condizione che la convenzione sia redatta conformemente alle presenti linee guida.

b) la convenzione ha per oggetto l'accesso a altre tipologie di dati, non rientranti nell'ambito di applicazione del D. Lgs. 30 giugno 2003, n. 196; in tale situazione, naturalmente, non è necessario dare corso al suddetto adempimento.

In relazione a quanto sopra, l'erogatore dovrà in ogni caso evidenziare la procedura di riferimento adottata. A tal fine la convenzione stessa conterrà una esplicita "autocertificazione" di conformità alle presenti linee guida.

Diversamente, nel caso in cui una convenzione, ovvero le modalità di accesso ad una determinata banca dati, siano già state oggetto di esame da parte del Garante per la protezione dei dati personali nell'ambito di specifici procedimenti, la convenzione stessa conterrà l'indicazione del parere o del provvedimento del Garante.

Come previsto dal successivo comma 3 dello stesso articolo 58, l'Agenzia per l'Italia Digitale provvede al monitoraggio in merito alla concreta attuazione della norma in questione, riferendo annualmente con apposita relazione al Ministro per la Pubblica amministrazione e alla Commissione per la valutazione, la trasparenza e l'integrità della amministrazioni pubbliche.

Nel richiamare l'attenzione in merito a quanto disposto dall'art. 12, co. 1-ter e dall'art. 52, co. 4, del CAD in merito alla concreta attuazione delle disposizioni di cui trattasi e della conseguente rilevanza ai fini della misurazione e valutazione della performance dirigenziale, si riassumono di seguito i passi fondamentali per l'attuazione della norma stessa:

1. ogni Amministrazione deve individuare le banche dati che possono essere oggetto di convenzione ai sensi dell'art. 58, CAD;

2. la stessa amministrazione, in qualità di erogatore, predispone lo schema di convenzione-quadro per ogni singola banca dati seguendo le indicazioni contenute nelle presenti linee guida, nel rispetto, in particolare, degli aspetti di sicurezza e privacy, riportati nel par. 5;

3. come sopra riportato, la convenzione conterrà l'autocertificazione della piena conformità della convenzione stessa alle presenti linee guida, ovvero l'indicazione del parere o del provvedimento del Garante per la protezione dei dati personali;

4. l'erogatore provvede a pubblicare detta convenzione-quadro nel proprio sito istituzionale, nella sezione "Amministrazione trasparente" seguendo la struttura definita dal D. Lgs. n. 33/2013, riportata nel par. 4, dandone comunicazione via PEC (protocollo@pec.agid.gov.it) all'Agenzia per l'Italia Digitale. La stessa Agenzia potrà effettuare controlli a campione sulle convenzioni-quadro dichiarate conformi alle presenti linee guida al fine di verificarne eventuali difformità, segnalandole all'erogatore. Se tali difformità sono relative agli aspetti di sicurezza e privacy, esse saranno notificate dall'Agenzia anche al Garante per la protezione dei dati personali per i successivi adempimenti. Restano ferme le eventuali prescrizioni ad hoc del Garante e gli eventuali controlli operati dal Garante stesso ai sensi del D. Lgs. n. 196/2003;

5. in relazione alle esigenze istituzionali dei potenziali fruitori e alla accertata sussistenza della base normativa che legittima tali esigenze, l'erogatore e il fruitore procedono alla stipula della convenzione;

6. l'erogatore comunica ufficialmente all'Agenzia per l'Italia Digitale (tramite protocollo telematico attraverso la casella PEC censita nell'indice delle PA) l'avvenuta stipula della convenzione, ai fini di quanto previsto dall'art. 58, comma 3, CAD. In particolare, per ogni convenzione stipulata l'erogatore dovrà fornire le seguenti informazioni come riportato nel seguente schema:

Erogatore	Banca dati di riferimento	Fruitore	Norme legittimanti l'accesso	Tipo di accesso/servizio	Data convenzione	Durata

Tale comunicazione non è necessaria nei casi in cui la fruizione dei dati avvenga in modalità di cooperazione applicativa. In questo caso

utilizzando i servizi previsti dal DPCM 1 aprile 2008 recante "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività", tale adempimento sarà soddisfatto attraverso la pubblicazione dell'accordo di servizio nel registro SICA (Servizi infrastrutturali di interoperabilità, cooperazione e accesso).