Garante privacy su sistema di gestione della fiscalità

Data 16 aprile 2014
Categoria Professione

Parere del Garante sull'affidamento, secondo il modello in house, della gestione del sistema informativo della fiscalità alla Sogei S.p.a. - 13 febbraio 2014

Registro dei provvedimenti
n. 68 del 13 febbraio 2014

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 e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere del Ministero dell'economia e delle finanze del 16 novembre 2013 (prot. n. 26208);

Visto il Codice in materia di protezione dei dati personali, d.lgs. 30 giugno 2003, n. 196 (di seguito Codice), con particolare riferimento all' art. 154, comma 1, lett. g);

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

Il Ministero dell'economia e delle finanze (di seguito Ministero), in vista della scadenza del Contratto di servizi quadro in vigore per il periodo 1 gennaio 2006 - 31 dicembre 2011, regolante il rapporto per la gestione in house del sistema informativo della fiscalità tra l'Amministrazione finanziaria nel suo complesso e la SOGEI S.p.A., quale suo ente strumentale preposto al settore dell'Information and Communication Technology, in data 20 dicembre 2011, ha inviato al Consiglio di Stato il nuovo schema di Contratto di servizi quadro 2012-2017, per il previsto parere obbligatorio.

Al fine di assicurare la continuità operativa e gestionale del sistema informativo della fiscalità, il legislatore ha prorogato gli istituti contrattuali in essere fino al completamento dell'iter di stipula del nuovo Contratto quadro (art. 5 del decreto-legge 2 marzo 2012, n. 16, convertito dalla legge 26 aprile 2012, n. 44).

Il Consiglio di Stato ha sospeso l'espressione del parere chiedendo di acquisire preventivamente i pareri dell'Autorità garante della concorrenza e del mercato, dell'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture e dell'Autorità per la protezione dei dati personali nonché del Ministero dell'istruzione, dell'università e della ricerca (MIUR) in quanto amministrazione che esercita la potestà di organizzazione e controllo su DigitPA. (parere del Consiglio dei Stato – Sez. II - n. 1891/2012 del 1 gennaio 2012).

In particolare, il Consiglio di Stato chiede di conoscere l'avviso di questa Autorità "per quanto riguarda le garanzie che devono essere prestate in ordine alla riservatezza dei dati raccolti nel corso della gestione dei servizi da parte della SOGEI".

In proposito, il Ministero, per le valutazioni di questa Autorità ha messo a disposizione la seguente documentazione:

•nuovo schema di Contratto di servizi quadro 2012-2017, comprendente due allegati: allegato 1 "Descrizione dei servizi" e allegato 2 "Programma di attuazione, Piano operativo, Soluzione operativa, Indicatori, Pianificazione dei pagamenti";
•parere di congruità tecnico-economico, rilasciato dall'Agenzia per l'Italia digitale.
Il Ministero, più precisamente, ha illustrato talune specifiche disposizioni del nuovo Contratto quadro evidenziando in particolareche:

•l'articolo 18 (Sicurezza del Sistema) reca disposizioni che impegnano la SOGEI ad assicurare adeguati livelli di sicurezza fisica e logica del Sistema informativo della fiscalità. A tale scopo, tenuto conto dei livelli di qualità dei servizi richiesti, la Società dovrà operare attraverso l'adozione di idonee misure organizzative, tecniche ed operative, per la protezione dei dati e delle informazioni gestiti, delle apparecchiature e dei sistemi di elaborazione utilizzati, nonché delle reti di comunicazione;
•l'articolo 19 (Prevenzione dei rischi) consente all'Amministrazione, attraverso l'attivazione di specifici audit, di verificare

l'attuazione di tutte le misure di sicurezza e prevenzione dei rischi legati a malfunzionamenti del sistema informativo, nell'ambito delle quali rientrano anche le misure volte a garantire il rispetto della normativa in materia di trattamento dei datipersonali;
•l'articolo 20 (Tutela dei dati personali e riservatezza), nel sottolineare che la SOGEI dovrà attenersi alle disposizioni del decreto legislativo n. 196/2003 e successive modificazioni ed integrazioni, secondo le istruzioni impartite dai responsabili delle Strutture Organizzative dell'Amministrazione finanziaria, in qualità di titolari del trattamento dei dati per le Strutture organizzative stesse, reca specifici obblighi e responsabilità in capo alla Società stessa.
Il Ministero, inoltre, ha messo in evidenza che:

•le Strutture organizzative dell'amministrazione finanziaria hanno nominato Sogei Responsabile esterno del trattamento dei dati personali, relativamente alle attività previste nel Contratto Quadro, nei contratti esecutivi e nei piani operativi annuali;
•le attività demandate a Sogei in ambito sicurezza e privacy "si esplicano essenzialmente lungo due direttrici: l'attuazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di ispirazione ISO 27001, e la definizione di un Sistema di Gestione della Privacy per l'attuazione delle norme e dei provvedimenti emessi dall'autorità Garante per la protezione dei dati personali".
•con decreto del Direttore Generale delle Finanze n. 2439 del 14 ottobre 2011, è stato istituito il Comitato per la sicurezza ICT e costituito il Comitato di governo del Sistema informativo della fiscalità, presieduti dal titolare della Direzione Sistema Informativo della Fiscalità, aventi, tra l'altro, rispettivamente, il compito di proporre regole e criteri da adottare per la sicurezza e la riservatezza delle informazioni, attraverso l'adozione di regole comuni per l'accesso ai dati, e il compito di presidiare i predetti indirizzi e strategie anche in materia di coordinamento, monitoraggio e controllo delle attività concernenti la sicurezza fisica, logica ed organizzativa. In particolare, detto ultimo Comitato indirizza le strategie per la realizzazione del Sistema di disaster recovery, centrale e periferico;
il decreto-legge 6 luglio 2012, n. 95, convertito dalla legge 7 agosto 2012, n. 135, ha disposto un riassetto organizzativo complessivo dell'amministrazione finanziaria, che ha interessato anche le società in house Consip e Sogei.

Il Ministero ha infine evidenziato che, anche alla luce del nuovo assetto istituzionale, risulta necessario che l'amministrazione finanziaria rinnovi quanto prima il Contratto quadro con Sogei, quale atto normativo presupposto per l'affidamento in house delle attività informatiche alla medesima società.

OSSERVA

A. aspetti di carattere generale

Nel trattamento di dati personali connesso allo svolgimento dei propri compiti istituzionali, ciascun titolare, anche pubblico, può avvalersi del contributo di soggetti esterni, affidando ad essi determinate attività che restano nella sfera della titolarità dell'amministrazione stessa e che non comportano decisioni di fondo sulle finalità e sulle modalità di utilizzazione dei dati. In questo caso, è necessario che l'amministrazione – in qualità di titolare del trattamento – designi il soggetto esterno, preposto allo svolgimento di determinate attività che comportano il trattamento di dati personali, come "responsabile del trattamento", con un apposito atto scritto che specifichi analiticamente i compiti ad esso affidati (artt. 4, c. 1, lett. f) e g), 28 e 29 del Codice).

In ogni caso, le persone fisiche che, anche presso il soggetto esterno, materialmente trattano i dati personali devono essere designate, dal titolare o dal responsabile, "incaricati del trattamento" con un atto scritto che individui puntualmente l'ambito del trattamento che essi possono effettuare (art. 30 del Codice).

In relazione alla questione in esame e ai fini del rispetto della normativa richiamata, l'Amministrazione finanziaria ha designato Sogei S.p.a., per lo svolgimento di determinate attività che comportano il trattamento di dati personali, quale "responsabile del trattamento dei dati personali". Tale designazione implica che Sogei sia stata individuata "tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza".

In tale quadro, con specifico riferimento al profilo della sicurezza di cui la società designata responsabile deve fornire idonee garanzie, sulla base della sopra richiamata documentazione messa a disposizione per la valutazione dell'Autorità, è possibile ricavare alcune indicazioni che appare opportuno rappresentare al Ministero, in relazione, in primo luogo, alla estrema delicatezza dei dati personali trattati nell'ambito del sistema informativo della fiscalità, nonché al rilevante importo dell'affidamento (2,5 miliardi di euro).

Più precisamente, tra le funzioni oggetto del contratto sono comprese la gestione della rete interna (Allegato 1, par. 10), la gestione dei collegamenti Internet (Allegato 1, par. 11), la funzione SOC security operation center (Allegato 1, par. 12), la gestione dei sistemi di identity and access management (Allegato 1, par. 13).

Si tratta di delicate componenti tecnologiche, trasversali rispetto ai diversi sottosistemi, su cui si basa la sicurezza dell'infrastruttura di erogazione, la capacità reattiva a incidenti e malfunzionamenti, la capacità di identificare l'utenza e assegnare i corretti diritti di accesso e profili di autorizzazione.

Costituiscono oggetto del contratto anche lo sviluppo e la manutenzione del software applicativo (sia di tipo custom sia basato su soluzioni di mercato) (Allegato 1, par. 2) nonché la conduzione dei server centrali a tecnologia legacy e quelli di tipo open, nonché i sottosistemi di storage. Infine sono compresi nell'oggetto contrattuale anche l'erogazione del servizio di posta elettronica e la gestione degli asset informatici.

A fronte della complessità dei servizi, gli aspetti di sicurezza e protezione dei dati personali appaiono solo sommariamente trattati al punto e) delle premesse al contratto e nei successivi artt. 18 (Sicurezza del sistema), 19 (Prevenzione dei rischi) e 20 (Tutela dei dati personali e riservatezza).

La definizione concreta di tali aspetti è, per lo più, demandata ad atti e momenti successivi: la definizione delle regole e dei criteri per la sicurezza e la riservatezza delle informazioni sono affidate al Comitato Sicurezza ICT, istituito con decreto del Capo del Dipartimento dell'economia n. 2439 del 14 ottobre 2011, mentre l'individuazione delle esigenze di sicurezza è demandata alla fase di disegno della singola soluzione operativa, attraverso la stesura di specifici Programmi di attuazione/Piani operativi.

B. Profili di criticità

Con riferimento agli aspetti generali sopra richiamati, sono individuati, di seguito, taluni profili di criticità nell'attuale formulazione del contratto, concernenti i soli aspetti di competenza in materia di protezione dei dati personali e dei connessi profili relativi alle misure di sicurezza.

1. Certificazioni di sicurezza

Per quanto riguarda i servizi di sviluppo e manutenzione evolutiva del software ad hoc (par. 2, pag. 13, Allegato 1) e di personalizzazione del software di mercato (par 3, pag. 16, Allegato 1) viene richiamata la circostanza che Sogei S.p.A. sia dotata di un sistema di gestione della sicurezza delle informazioni e di un sistema di qualità dei dati conformi, ma non certificati da un organismo di certificazione, rispettivamente, allo standard ISO 27001:2005 e allo standard ISO 25012:2008.

Al riguardo, si ritiene opportuno che il Ministero, con specifico riferimento agli aspetti di protezione dei dati personali, richieda a Sogei, oltre alla dichiarazione di essere dotato di un sistema di qualità dei dati conforme allo standard ISO 27001:2005, anche la pronta predisposizione degli elementi per dare prova, a richiesta, di tale adempimento.

2. Servizi di sicurezza della rete

Mentre non costituisce oggetto di valutazione in questa sede l'adeguatezza, in generale, dei livelli di servizio (service level agreement o SLA) alla tipologia di prestazioni formanti oggetto dell'affidamento, occorre soffermarsi sulla loro rilevanza rispetto alla protezione dei dati personali per alcuni sottosistemi e servizi di rilevante importanza.

Ci si riferisce, in particolare, ai servizi di cui al par. 10, Allegato 1, per cui la disponibilità degli apparati di sicurezza contrattualmente prevista risulta del 95%, valore che, negli orari indicati, corrisponde ad una indisponibilità potenziale di quasi 3 ore a settimana lavorativa che non verrebbe rilevata come disservizio (cfr. tabella in par. 10, pag. 49 dell'Allegato1).

Si ritiene opportuno che a soglia sia riportata a valori idonei alla delicatezza del servizio, da cui dipende la sicurezza periferica dell'intera infrastruttura Sogei e della rete di accesso per il collegamento degli enti esterni.

Anche i connessi "tempi di risposta a richieste di implementazione di regole di sicurezza" (nella stessa tabella citata) è opportuno che vengano ricondotti a valori più stringenti, per consentire di adeguare le misure di protezione perimetrale al variare delle minacce, in luogo delle 16 ore lavorative dalla richiesta (corrispondenti a due giornate lavorative).

La disponibilità e i tempi di ripristino degli apparati di sicurezza sono poi rilevati, al fine di verificare il rispetto degli SLA contrattuali, nella fascia oraria lunedì-venerdì 8,00 – 18,00, sabato 8,00-14,00, a fronte di servizi erogati in modalità H24, scelta che può condurre a misurazioni fortemente sovrastimate degli indici di prestazione anche in presenza di esteseinterruzioni.

In tale quadro, quindi, deve essere chiarito che il rispetto degli SLA contrattuali relativi a servizi di sicurezza in modalità H24 sia verificato nell'intero arco temporale di erogazione; ciò, al fine di evitare che non risulti possibile contestare violazioni degli SLA e applicare penali anche in casi di prolungate interruzione dei servizi, che non verrebbero rilevate.

3. Gestione della navigazione su rete Internet

Relativamente al par. 11.1, pag. 51 dell'Allegato 1, si osserva che sono previsti nel contratto servizi di filtraggio della navigazione sulla rete Internet con protocolli http ed https e tecniche di white listing statico e dinamico.

Al riguardo, deve essere assicurato il rispetto del provvedimento di questa Autorità sull'uso di posta elettronica e Internet sul luogo di lavoro, evitando la raccolta di dati eccedenti in forma di log files delle richieste provenienti dalle reti interne (Provv. 1° marzo 2007, G.U. n. 58 del 10 marzo 2007, disponibile sul sito istituzionale www.garanteprivacy.it).

4. Livelli di servizio per Identity access management

Relativamente ai servizi di identity management di cui al par. 13.1, pag. 55 dell'Allegato 1, a fronte di un'erogazione di tipo H24 è previsto un livello di disponibilità del servizio del 95%, che appare inadeguato. Il sistema è infatti una componente determinante della sicurezza dell'infrastruttura, e la sua indisponibilità potrebbe avere effetti sulla capacità di intervenire sui diritti di accesso per adeguarli a mutate e anche urgenti esigenze (si pensi alla necessità di abilitare o

disabilitare determinati profili di autorizzazione o utenze).

Il valore soglia indicato appare eccessivamente basso e le modalità della sua rilevazione (mensile, su 56 ore settimanali) lascia spazi ad ampie interruzioni che non verrebbero contrattualmente rilevate come disservizio. Tale valore, pertanto, è opportuno che venga adeguato al fine di evitare le predette disfunzioni.

5. Conduzione centrale (mainframe, server, storage) e disaster recovery

I livelli di servizio indicati relativamente al disaster recovery non si possono ritenere adeguati alla molteplicità dei sottosistemi, alcuni dei quali con un elevato livello di criticità, che compongono il sistema informativo della fiscalità.
In particolare, destano perplessità i seguenti livelli di servizio (cfr. par. 7, pag. 36, allegato 1), che prevedono:

•Sito di disaster recovery indisponibile fino a 2,4 giorni a quadrimestre (disponibilità dichiarata del 98% su base quadrimestrale);
•Copia on-line dei dati in modalità asincrona senza dettagli sui tempi di latenza;
•Verifica della correttezza del disaster recovery ogni 6 mesi.
Si ritiene opportuno indicare al Ministero di valutare l'innalzamento dei precedenti SLA, almeno per un sottoinsieme di sistemi/servizi ritenuti critici, e di ridurre il tempo intercorrente tra verifiche successive della correttezza del disaster recovery.

Più in generale, si ritiene opportuno richiamare il Ministero alle prescrizioni di cui all'art. 50-bis del Codice dell'amministrazione digitale (d.lgs. n. 82/2005), relative all'adozione del piano di Continuità operativa e di disaster recovery, da redigersi sulla base dello studio di fattibilità tecnica approvato dall'Agid, e di includere la business continuity tra gli obiettivi di controllo previsti dallo standard 27001:2005.

6. Gestione degli incidenti informatici

Un'attenzione particolare in un sistema tecnologico di grandi dimensioni come quello in esame richiede il monitoraggio e il trattamento degli incidenti relativi alla sicurezza delle informazioni.

In particolare, per quanto riguarda eventuali violazioni di dati personali (si pensi ad attacchi informatici, incendi o altre calamità, che possano comportare la perdita, la distruzione o la diffusione indebita di dati (c.d."data breach") è opportuno prevedere, in sede contrattuale, l'obbligo per il responsabile di comunicare tempestivamente all'Amministrazione committente gli elementi dai quali possa valutare compiutamente la gravità dell'evento verificatosi, anche in ragione del numero dei soggetti coinvolti e della quantità e qualità dei dati colpiti, l'entità del danno cagionato e le misure adottate per ridurlo.

TUTTO CIO' PREMESSO IL GARANTE

con riferimento alla richiesta del Ministero dell'economia e delle finanze in ordine alla possibilità di procedere all'affidamento, secondo il modello in house, della gestione del sistema informativo della fiscalità alla Sogei S.p.a., esprime parere, in relazione ai soli profili di competenza concernenti la disciplina in materia di protezione dei dati personali, nei termini di cui in motivazione (art. 154, comma 1, lett. g) del Codice).

Roma, 13 febbraio 2014

ILPRESIDENTE
Soro

ILRELATORE
Soro

IL SEGRETARIO GENERALE
Busia

Il provvedimento:
[url]http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3001879[/url]