Anagrafe tributaria: sicurezza e accessi - 18 settembre 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 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 prof. Francesco Pizzetti;

PREMESSO

Sulla base di un'analisi preliminare del sistema informativo della fiscalità, il 14 dicembre 2007 il Garante ha deliberato l'avvio di accertamenti volti a verificare, in più fasi, i trattamenti di dati personali effettuati presso l'anagrafe tributaria, rilevando che elementi di maggior criticità e urgenza erano da ravvisarsi nelle misure di sicurezza adottate per gli accessi da parte di enti esterni, pubblici e privati, all'amministrazione finanziaria.

La prima fase di accertamenti attinente a tali accessi è stata completata. Il Garante svolgerà nel prosieguo le altre verifiche programmate sul trattamento dei dati effettuato dalle articolazioni dell'amministrazione finanziaria, con particolare riguardo alla struttura degli archivi, alle modalità di accesso, alle applicazioni utilizzate, alle tipologie di informazioni, alle misure di sicurezza, alle abilitazioni e alle autorizzazioni degli utenti.

Le attività ispettive completate hanno invece riguardato, in particolare:

1) il controllo degli applicativi che consentono l'accesso all'anagrafe tributaria a soggetti esterni all'amministrazione finanziaria (loro funzionalità; tipologie di dati visualizzabili con i differenti profili di autorizzazione previsti);

2) la designazione di responsabili e di incaricati, i sistemi di autenticazione (ad es., modalità di formazione e gestione delle *password*; controlli degli accessi ai sistemi applicativi) e i sistemi di autorizzazione;

3) le procedure di *audit* interno ed esterno sull'accesso alle informazioni contenute nell'anagrafe tributaria (ad es., controlli sulle abilitazioni e sulle autorizzazioni degli utenti abilitati all'utilizzo degli applicativi, modalità di raccolta dei *logfile* e loro analisi automatizzata).

Gli accertamenti ispettivi hanno avuto luogo presso l'Agenzia delle entrate, Sogei S.p.A. (Società generale d'informatica, responsabile del trattamento dei dati contenuti nell'anagrafe tributaria), regioni, province, comuni e altri enti che accedono a tale anagrafe, con la piena collaborazione degli enti coinvolti. Le verifiche hanno consentito di evidenziare criticità, in ambito sia informatico, sia organizzativo, documentate nei verbali in atti.

Dalle risultanze emerge che i sistemi di collegamento all'anagrafe tributaria utilizzati dai soggetti esterni all'amministrazione finanziaria sono i seguenti:

- "Siatel", applicazione *web* utilizzata principalmente da comuni, province, regioni, università, asl e consorzi di bonifica, per un totale di circa 9.400 enti e 60.000 utenze, che consente di visualizzare dati anagrafici completi, dati fiscali e atti del registro relativi alla totalità dei contribuenti;
- "Puntofisco", applicazione *web* di recente realizzazione e attualmente in dotazione a enti previdenziali, tribunali, camere di commercio e società varie, per un totale di circa 180 enti e 18.000 utenze. Puntofisco consente di visualizzare dati anagrafici, fiscali e atti del registro relativi alla totalità dei contribuenti, più aggiornati e con maggiore segmentazione delle informazioni rispetto a Siatel (ad es., differenziando tra dati anagrafici attuali o completi dello storico), ma permette anche di accedere a dati sensibili (presenti nel dettaglio degli oneri deducibili);
- "3270 enti esterni", collegamento diretto, tramite terminali fisici o emulatori di terminale, ai sistemi centrali dell'anagrafe tributaria, in corso di dismissione per esigenze di aggiornamento tecnologico, che tuttora consente a soggetti anche privati (Telecom Italia S.p.A., Enel, Inail, Inps, camere di commercio, Ministero delle politiche agricole, *"interforze"*) di collegarsi a informazioni anagrafiche e fiscali relative alla totalità dei contribuenti; la struttura dell'applicativo non consente all'Agenzia delle entrate di conoscere il numero di utenti;
- "Entratel", applicativo utilizzato dagli enti principalmente ai fini della trasmissione delle dichiarazioni, con flussi di dati solo in entrata verso l'Agenzia delle entrate; le credenziali di autenticazione fornite dall'Agenzia permettono altresì all'operatore di visualizzare la posizione fiscale dell'ente attraverso l'apposita *web application* ("Fisconline"/"Cassetto fiscale");
- *"web services"*, strumenti realizzati sulla base di specifiche tecniche definite caso per caso dall'Agenzia delle entrate, che consentono di accedere a dati anagrafici anche completi relativi alla totalità dei contribuenti. Tali collegamenti sono utilizzati da 21 enti, ma la configurazione del collegamento non consente all'Agenzia di conoscere il numero di utenti;
- *"file transfer"*, collegamenti per la gestione di flussi di dati per la gran parte in entrata (principalmente provenienti da banche), ma alcuni anche in uscita (ad es., verso concessionari della riscossione), utilizzati da circa 200 enti.

OSSERVA

Nel corso dei menzionati accertamenti ispettivi, sulla base della documentazione in atti, sono state riscontrate alcune criticità di seguito descritte, già in parte riconosciute dall'Agenzia, relative agli accessi all'anagrafe tributaria da parte degli enti esterni all'amministrazione finanziaria, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati. Accanto a diverse problematiche attinenti alla sicurezza, sono emersi e vengono affrontati connessi profili concernenti aspetti sostanziali del trattamento.

Il Garante, ai sensi dell'art. 154, comma 1, lett. c) del Codice, ritiene necessario prescrivere una serie di misure e accorgimenti che devono essere adottati dall'Agenzia delle entrate, anche in riferimento ai soggetti esterni che accedono all'anagrafe tributaria, di seguito indicati. Tali misure e accorgimenti, principalmente di carattere tecnico e organizzativo, sono necessari al fine di porre rimedio alle carenze riscontrate e a incrementare, in particolare, i livelli di sicurezza degli accessi all'anagrafe tributaria, rendendo il trattamento conforme alle disposizioni vigenti.

1. Accessi all'anagrafe tributaria da parte di soggetti esterni all'amministrazione finanziaria: profili generali

Criticità

Alcuni accertamenti in proposito sono risultati meno agevoli in considerazione del fatto che l'Agenzia non aveva immediatamente disponibile, come richiesto dall'Autorità, una completa documentazione relativa sia ai soggetti esterni collegati, sia ai sistemi di accesso utilizzati da questi ultimi (numero e categorie di soggetti, finalità degli accessi e tipologie di collegamenti e di dati comunicati).

Dagli atti emerge ora che l'Agenzia autorizza gli accessi all'anagrafe tributaria solo in seguito alla stipula di apposite convenzioni, anche *standard*, a livello centrale e regionale. Tuttavia, l'assenza di una documentazione di insieme sui collegamenti in essere non agevola un monitoraggio costante sulla sussistenza dei presupposti che hanno consentito l'attivazione del canale informativo, nonché i dovuti controlli sulla correttezza della gestione degli accessi e della consultazione delle informazioni. La periodica ricognizione degli enti che accedono all'anagrafe tributaria, e dei rispettivi utenti, costituisce infatti la premessa per prevenire usi impropri e illeciti delle informazioni in essa contenute.

È stato inoltre riscontrato in atti che in alcune convenzioni stipulate per l'accesso all'anagrafe tributaria non risultano delimitate chiaramente le finalità per cui gli accessi vengono autorizzati; sotto tale aspetto, è stato rilevato che alcuni enti, attraverso gli amministratori locali (soggetti deputati all'abilitazione degli utenti), hanno abilitato di propria iniziativa alcuni utenti al fine di attivare nuovi flussi di dati per finalità ulteriori rispetto a quelle consentite.

Non risulta altresì dagli atti che gli operatori che effettuano gli accessi abbiano l'onere (o la possibilità) di registrare, anche al fine di successivi controlli, le ragioni a supporto delle interrogazioni eseguite.

È stato inoltre verificato che i dati visualizzabili attraverso gli applicativi non sono segmentabili in relazione al bacino di utenza dell'ente che chiede il collegamento (ad es., territorio comunale), e sono relativi a tutto il territorio nazionale.

Infine, le informazioni consultabili non risultano, talvolta, sufficientemente aggiornate per lo svolgimento delle funzioni istituzionali cui gli accessi sono finalizzati (ad es., in Siatel, ai fini della verifica dell'Isee non sono visualizzabili i dati dell'ultima dichiarazione presentata e vengono invece visualizzati dati reddituali riferiti ad annualità pregresse, eccedenti e non pertinenti rispetto alle finalità perseguite, che non consentono di effettuare i puntuali controlli sulle autocertificazioni reddituali ai sensi del d.P.R. n. 445/2000).

Da ultimo, sulla base delle risultanze in atti, è stato rilevato che gli accessi all'anagrafe tributaria vengono effettuati talvolta per conoscere informazioni (ad es., la residenza) che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti (ad es., amministrazioni certificanti ai sensi dell'art. 71 del d.P.R. n. 445/2000).

Prescrizioni

L'Agenzia deve disporre di informazioni complete e strutturate sulla molteplicità di soggetti che, a vario titolo, accedono alla banca dati dell'anagrafe tributaria. Occorre pertanto che la stessa rediga un documento, con formalità descrittive *standard*, che riporti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattivo, *batch* o di altro genere, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a realizzarlo, la base normativa (anche ai sensi dell'art. 19, comma 2 del Codice, previa comunicazione al Garante), la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza e il volume dei

trasferimenti o degli accessi e il numero di soggetti che utilizzano la procedura. Tale documento dovrà essere mantenuto costantemente aggiornato, nonché reso disponibile nel caso di controlli.

L'Agenzia deve altresì verificare, con cadenza periodica annuale, l'attualità delle finalità per cui ha concesso l'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice (norme di legge o regolamento, nonché eventuali comunicazioni al Garante ai sensi dell'art. 19 del Codice) e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscere informazioni che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti.

Per vincolare effettivamente gli accessi alle finalità consentite, l'Agenzia deve introdurre nelle applicazioni volte all'uso interattivo da parte di incaricati 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.

L'Agenzia deve poi far sì che gli applicativi consentano, per quanto più possibile, la segmentazione dei dati visualizzabili -in particolare in modo cronologico (attuale o storico, per periodi di imposta), geografico (comune, provincia, regione) e per tipologia di dati (ad es. di sintesi)- al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza dell'ente che chiede il collegamento, esclusivamente i dati necessari rispetto alle finalità perseguite (ad es. l'ultimo domicilio fiscale o l'ultimo periodo di imposta).

2. I sistemi utilizzati per il collegamento all'anagrafe tributaria

2.1. Profili comuni

Le principali criticità di carattere generale relative all'utilizzo degli applicativi riscontrate nel corso degli accertamenti ispettivi sugli accessi da parte dei soggetti esterni sono di seguito individuate.

2.1.1. Sicurezza dei sistemi di autenticazione

Criticità

Per le *web application* è stato utilizzato un certificato *Ssl* di tipo *self signed* (non firmato da una *Ca, Certification authority*, ufficiale) non attendibile che, in mancanza di una *Ca* affidabile, non offre le garanzie di certezza dell'identità dell'erogatore del servizio tipiche della certificazione digitale tramite *Pki (public key infrastructure*): risultano pertanto facilitate azioni di *phishing* in danno di utenti del sistema e la possibile acquisizione indebita di credenziali di autenticazione, idonea a consentire utilizzi impropri dell'applicazione.

Dalle risultanze agli atti emerge inoltre che, rispetto a taluni collegamenti, l'identificazione dell'utente finale dell'applicazione è in molti casi in capo all'ente esterno. L'Agenzia non ha pertanto alcuna conoscenza dell'effettiva identità e del numero degli utenti che accedono, con tali modalità di connessione, da sistemi informativi esterni collegati direttamente all'anagrafe tributaria (ad es., 3270 enti esterni e *web services*).

È risultato, poi, possibile accedere alle *web application* Siatel e Puntofisco attraverso l'utilizzo delle medesime credenziali contemporaneamente da postazioni diverse, anche con indirizzo *Ip* diverso (perfino da rete esterna all'ente), nonostante, per quanto riguarda il Siatel, all'atto dell'accesso tale possibilità venga esclusa da un apposito avviso.

Prescrizioni

L'Agenzia deve prevedere che tutte le applicazioni accessibili da rete pubblica in forma di *web application* siano implementate con protocolli *https/ssl* provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una *Certification Authority* ufficiale, evitando il ricorso a certificati di tipo *self-signed*.

Allo scopo di identificare le postazioni da cui vengono effettuati gli accessi, occorre inoltre che l'Agenzia implementi un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che, basandosi sul mutuo riconoscimento tra i *server* che erogano il servizio e le postazioni che accedono a esso, consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

A fronte dell'accertata possibilità per taluni applicativi di effettuare più accessi contemporanei con le medesime credenziali, al fine di consentire a ciascun utente di controllare l'utilizzo del proprio *account*, l'Agenzia deve poi prevedere -in considerazione della specificità dell'anagrafe tributaria- la visualizzazione, nella prima schermata successiva al collegamento, di 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). Per accrescere la consapevolezza del controllo, le stesse informazioni devono essere riportate anche relativamente alla sessione corrente.

Infine, l'Agenzia deve disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali (sessioni multiple), limitandone l'utilizzo ai soli casi necessari per esigenze di servizio (ad es., per le connessioni originate da una stessa postazione di lavoro). In ogni caso, tale possibilità deve essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti, come sopra descritto. Nel caso in cui non sia possibile individuare la postazione di lavoro, nelle more dell'attuazione delle prescrizioni sopra individuate, deve essere inibita la possibilità di accessi contemporanei.

2.1.2. Amministratori locali, abilitazioni e autorizzazioni

Criticità

È stato verificato negli accertamenti ispettivi che gli enti esterni hanno spesso affidato il compito di amministratore locale (il soggetto deputato alla gestione delle utenze) a personale non in grado né di valutare la pertinenza delle richieste di abilitazione delle utenze, né di monitorarne gli eventuali utilizzi impropri. In taluni enti è stata riscontrata la presenza di più amministratori locali con funzionalità che non consentivano di gestire gli utenti in modo tra loro coordinato.

Dalle risultanze agli atti è emerso, inoltre, che non è stato predeterminato un adeguato flusso informativo tra l'amministratore locale e l'unità organizzativa deputata alla gestione del personale al fine di consentire l'immediata disabilitazione o revisione del profilo di autorizzazione dei soggetti indirizzati ad altre mansioni o il cui rapporto con l'ente sia cessato.

Sono stati riscontrati poi casi di cessioni e condivisioni di credenziali di accesso, profili di autorizzazione inadeguati e/o eccessivi rispetto alle finalità perseguite, nonché mancate designazioni di incaricati al trattamento.

É stato verificato altresì che alcuni enti hanno utilizzato strumenti automatizzati di interrogazione che hanno consentito la duplicazione anche massiva di dati contenuti nell'anagrafe tributaria, con la

creazione di autonome basi di dati, non conforme alle finalità per le quali è stato autorizzato l'accesso all'anagrafe tributaria.

Dalla documentazione in atti emerge che l'Agenzia, anche a seguito delle prime risultanze dell'attività ispettiva sopra illustrate, ha manifestato l'intenzione di voler gestire direttamente l'abilitazione di tutte le utenze, eliminando gli amministratori di sistema degli enti esterni.

Al riguardo, nonostante le predette criticità concernenti l'attività svolta dagli amministratori esterni, il modello decentrato di gestione delle utenze incentrato su tali figure, opportunamente integrato con le misure di seguito descritte, costituisce comunque il perno per un corretto sistema di accesso all'anagrafe tributaria. L'amministratore locale, infatti, è il soggetto più idoneo a controllare l'attività quotidiana dei propri utenti senza limitarne l'operatività, anche a fronte dell'ingente numero di enti, e quindi di utenti, abilitati ad accedere all'anagrafe tributaria, ognuno per il proprio specifico fabbisogno informativo.

Prescrizioni

L'Agenzia, nelle convenzioni che disciplinano l'accesso all'anagrafe tributaria, deve prevedere che gli "amministratori locali" (soggetti deputati alla gestione delle utenze) scelti dagli enti esterni siano individuati sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Questi soggetti, prima di intraprendere la loro attività, devono essere formati dall'Agenzia delle entrate in ordine alle funzionalità dell'applicativo e all'attività di autorizzazione degli utenti. L'amministratore locale dell'ente esterno che accede all'anagrafe tributaria deve rimanere il punto di riferimento per le richieste di abilitazione e autorizzazione con la possibilità di gestire direttamente le utenze; deve essere altresì dotato degli adeguati strumenti di controllo sugli accessi (cfr. punto 3).

Nelle convenzioni deve essere poi previsto che gli enti esterni, anche per mezzo degli amministratori locali, debbano istruire adeguatamente il personale addetto all'utilizzo dei vari applicativi in ordine al corretto utilizzo delle funzionalità dei *software*. Le convenzioni, entro i medesimi termini, devono inoltre imporre periodici controlli sugli accessi agli enti esterni -anche attraverso gli appositi strumenti di monitoraggio e *alert* in dotazione all'amministratore locale che saranno attivati dall'Agenzia (cfr. punto 3)- i cui esiti devono essere documentati secondo le modalità definite nelle convenzioni stesse.

Le convenzioni devono anche predefinire una procedura per le autenticazioni e le autorizzazioni 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 l'amministratore tecnicamente deputato alla materiale gestione delle abilitazioni (e del relativo profilo), ma deve rispondere del controllo sullo stesso. Occorre inoltre che venga assicurato un flusso di comunicazione tra l'amministratore locale 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 (soprattutto con riguardo ad enti di rilevanti dimensioni), anche con apposite verifiche a cadenza almeno trimestrale.

Per quanto riguarda la possibilità di individuare più amministratori locali per ciascun ente, l'Agenzia deve valutare e coordinare attentamente i profili di autorizzazione da attribuire, garantendo in capo a un'unica figura la possibilità, ove occorra, di intervenire su tutti gli utenti anche amministratori, monitorandone l'operato (amministratore con ruolo di supervisore).

É necessario che l'Agenzia predefinisca anche soglie relative al numero di utenti abilitabili da ciascun ente in relazione alle sue dimensioni e alle finalità per le quale viene richiesto il collegamento. Le richieste di superamento di tali soglie devono essere valutate caso per caso dall'Agenzia stessa.

Le *web application* predisposte dall'Agenzia per l'utilizzo da parte di enti esterni vanno integrate con procedure di "autenticazione forte" (*strong authentication*) per ridurre la possibilità di usi impropri delle credenziali, la loro cessione o la loro sottrazione ai legittimi assegnatari. Tali procedure devono essere prefigurate nei confronti delle classi di utenti cui corrispondono profili di autorizzazione più critici in relazione alle funzioni o ai dati accessibili e, comunque, almeno per tutti i profili di autorizzazione corrispondenti alle funzioni di amministrazione locale delle applicazioni. Tali procedure potranno essere basate sull'utilizzo di dispositivi standard quali *smart card* o *token* per la generazione di *one-time-password*.

L'Agenzia deve infine prevedere limitazioni orarie per gli accessi, mantenendo la possibilità di specifiche deroghe adeguatamente motivate.

Le convenzioni stipulate con ciascun ente devono prevedere espressamente i vincoli necessari ad assicurare un corretto trattamento dei dati e devono stabilire le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione.

2.2. I singoli sistemi

2.2.1. Siatel

Criticità

Con particolare riferimento all'applicativo Siatel, nel corso degli accertamenti sono state rilevate le seguenti criticità:

- l'area di gestione dei file da scaricare nella funzione "fornitura dati" disponibile per i comuni e le regioni riporta soltanto la data di primo *download* del file, che rimane da quel momento disponibile per ulteriori e illimitati *download* non censiti e, pertanto, non controllabili;
- le funzionalità di *file transfer*, predisposte per i comuni ai fini dell'allineamento dell'anagrafe tributaria con le anagrafi della popolazione, sono state talvolta utilizzate per finalità diverse, potendo determinare l'introduzione di informazioni errate nei sistemi;
- i dati anagrafici visualizzabili sono completi (ad es., forniscono sempre lo "storico" delle residenze) e non è possibile limitare la consultazione alle sole informazioni anagrafiche attuali.

Prescrizioni

L'Agenzia deve introdurre misure di controllo per la funzionalità di "fornitura dati" visualizzabile nell'apposita schermata dell'applicativo (ad es., rimuovendo il *file* messo a disposizione in rete dopo un certo tempo dalla richiesta, ovvero indicando il numero di operazioni di *download* già effettuate per ciascun *file*, l'utenza, la data e l'orario del *download*, nonché limitandoli alla sola utenza richiedente).
Con riferimento alle funzionalità di Siatel utilizzabili da parte degli operatori comunali a soli fini anagrafici, devono essere inserite nell'applicativo da parte dell'Agenzia specifiche indicazioni all'amministratore locale affinché vengano autorizzati solo utenti che agiscono presso l'ufficio anagrafe del comune.

2.2.2. Puntofisco

Criticità

In relazione al sistema Puntofisco è stato verificato dalle risultanze in atti che l'applicativo permette di visualizzare i dati sensibili relativi agli oneri deducibili contenuti nelle dichiarazioni dei redditi.

L'amministratore locale ("gestore") non è in grado di visualizzare lo stato delle utenze (attiva/disattiva) e la lista utenti a lui disponibile comprende anche gli utenti già disabilitati. Il sistema di gestione delle utenze, inoltre, non permette regolarmente al gestore (amministratore), visualizzando il profilo dell'utente, di conoscere l'effettiva possibilità di accesso dello stesso al sistema.

Prescrizioni

Occorre aggiornare il profilo di autorizzazione assegnato agli enti esterni abilitati, escludendo a priori la consultabilità di dati sensibili laddove non sussista un'idonea base normativa che consenta la comunicazione di tale categoria di dati.

L'Agenzia deve inserire all'interno della procedura informatica di gestione degli utenti in uso all'amministratore locale indicazioni che gli consentano di visualizzare lo *status* di tutte le utenze con i profili abilitativi correnti, comprese quelle già cancellate. Deve essere corretta altresì l'anomalia, relativa al sistema di gestione, che non permette regolarmente all'amministratore locale, visualizzando il profilo del singolo utente, di conoscerne l'effettiva possibilità di accesso dello stesso al sistema.

2.2.3. 3270 enti esterni, web services e file transfer

Criticità

Con riferimento alle risultanze ispettive, è stato rilevato che il collegamento denominato 3270 enti esterni, l'accesso tramite *web service* e lo scambio dati mediante *file transfer* non consentono attualmente di limitare e controllare gli accessi in relazione alla loro provenienza, e non garantiscono misure idonee a verificare il rispetto delle regole di sicurezza di cui all'Allegato B del Codice. In particolare, è risultato che:

- l'Agenzia non è in grado di quantificare i soggetti che accedono ai dati, di attribuire agli stessi le operazioni tracciate dal sistema e di verificare il rispetto delle misure di sicurezza poiché l'identificazione degli *end-user* degli applicativi è affidata all'ente esterno che chiede il collegamento, come anche l'attribuzione certa a ogni incaricato di una o più credenziali per l'autenticazione, nonché la periodica scadenza della parola chiave;
- è impossibile per l'Agenzia individuare la postazione che effettua gli accessi, risultando assenti idonei sistemi che la consentirebbero quali, ad esempio, la certificazione digitale sulle postazioni e sugli emulatori di terminale utilizzati.

Prescrizioni

Devono essere garantite condizioni adeguate di protezione dei dati personali, di controllo e di verifica delle attività compiute (funzioni di *audit*) sugli applicativi utilizzati per accedere all'anagrafe tributaria, nonché strumenti che permettano all'Agenzia di verificare il rispetto delle misure di sicurezza.

Per quanto riguarda gli accessi all'anagrafe tributaria effettuati mediante l'applicativo 3270 enti esterni gli enti ad oggi abilitati devono migrare verso applicativi che offrono maggiori garanzie (ad es., Puntofisco o Siatel).

Con riferimento ai *web service*, l'Agenzia deve effettuare una ricognizione dei servizi al momento esposti e sospenderne l'attività in attesa della revisione delle attuali modalità di implementazione con le adeguate misure e gli accorgimenti di seguito descritti.

Laddove, infatti, l'Agenzia intenda impiegare *web service* esposti anche in una rete pubblica per l'utilizzo da parte di enti esterni, questi, in considerazione della delicatezza delle informazioni contenute nell'anagrafe tributaria, anche al fine di evitare duplicazioni delle banche dati e rischi di disallineamento, devono essere configurati offrendo un livello minimo di accesso ai dati e limitando i risultati delle interrogazioni a valori di tipo *booleano* (ad es., *web service* che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un determinato codice fiscale).

Le convenzioni per l'utilizzo di tali servizi, inoltre, devono prevedere stringenti condizioni d'uso tali da consentire anche un'effettiva capacità di controllo da parte dell'Agenzia. Dal punto di vista tecnico, tali condizioni d'uso dei *web service* devono essere trasposte in appositi "accordi di servizio", redatti secondo il modello della cooperazione applicativa impiegata all'interno del sistema pubblico di connettività istituito dal Codice dell'amministrazione digitale. Gli "accordi di servizio" devono individuare idonee garanzie per il trattamento dei dati personali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con possibilità di identificazione dell'utente che accede ai dati, il *timestamp*, l'indirizzo Ip di provenienza dell'utente e del *server* interconnesso, l'operazione effettuata e i dati trattati.

I collegamenti per la gestione di flussi di dati mediante *file transfer* devono essere realizzati su canali di connessione sicuri e l'Agenzia deve garantire, anche attraverso la configurazione dei sistemi, che le credenziali di abilitazione utilizzate dagli operatori dell'ente esterno rispettino le prescrizioni indicate nell'Allegato B al Codice, in particolare identificando il soggetto che effettua lo scambio dei dati e prevedendo che la parola chiave prevista sia soggetta a scadenza periodica secondo i termini ivi indicati.

2.2.4. Entratel

Criticità

Dagli accertamenti ispettivi è emerso che le caratteristiche tecniche di Entratel, in uso dal 1998, sono state realizzate al fine di consentire al tempo la massima fruibilità dell'applicativo anche a soggetti con limitate risorse tecnologiche. Allo stato degli atti, le credenziali attribuite dall'Agenzia (anche le chiavi asimmetriche) identificano però solo l'ente richiedente, anziché l'operatore finale. Per quanto riguarda l'accesso all'applicativo Fisconline/Cassetto fiscale, le *password* non sono soggette a scadenza periodica.

Prescrizioni

L'Agenzia deve configurare Entratel e Fisconline/Cassetto fiscale in modo da poter verificare il rispetto delle prescrizioni indicate nell'Allegato B al Codice relative, in particolare, al sistema di scadenza delle *password* e all'attribuzione di credenziali idonee ad identificare direttamente, oltre all'ente abilitato, anche il singolo incaricato che fisicamente effettua l'accesso, autentica e trasmette i *file*.

3. Le procedure di audit sull'accesso alle informazioni contenute nell'anagrafe tributaria da parte di soggetti esterni

Criticità

Gli accertamenti hanno permesso di verificare che tutti i *file* di *log* relativi alle transazioni effettuate nell'anagrafe tributaria sono conservati a tempo indeterminato da Sogei S.p.a., quelli relativi agli ultimi sette giorni sono mantenuti in linea, mentre quelli precedenti sono conservati su nastri magnetici.

Talvolta Sogei S.p.a., di propria iniziativa, al fine di monitorare anomalie e funzionalità del sistema, ha eseguito alcuni rilievi quantitativi sulle transazioni effettuate provvedendo a segnalare all'Agenzia le attività difformi riscontrate.

Secondo quanto si evince dalla documentazione in atti, l'Agenzia dispone di uno strumento di *business intelligence* denominato Vermont che, per quanto riguarda gli enti esterni, consente di controllare gli accessi effettuati dagli utenti con Siatel (e non quindi, in particolare, con Puntofisco e *web services*) dal 1° gennaio 2005 alle informazioni loro disponibili. Tale strumento permette poi monitoraggi statistici degli accessi e la predisposizione di sistemi di *alert*. Vermont utilizza *database* multidimensionali e consente di visualizzare i *log* relativi a un'interrogazione delle c.d. "informazioni generalizzate at" (principalmente, dati anagrafici e fiscali contenuti in anagrafe tributaria), mentre quelli relativi alle variazioni delle utenze o agli accessi a dati diversi, pur essendo registrati, non vengono rilevati da tale sistema. Analogo strumento è in dotazione anche a Sogei S.p.a.

Sulla base delle risultanze ispettive, è possibile rilevare tuttavia che l'Agenzia delle entrate non ha predisposto idonee procedure di *audit* anche periodiche sugli enti esterni.

Con particolare riferimento alle *web application* (Siatel e Puntofisco), non risultano monitorati l'attività degli amministratori locali, il numero di utenze abilitate da questi ultimi, i profili di autorizzazione e gli accessi; ciò, sebbene, per quanto riguarda Siatel, siano disponibili gli strumenti applicativi di gestione delle utenze (in uso alla Direzione centrale e alle direzioni regionali competenti) e il predetto sistema Vermont.

L'applicativo di *business intelligence* Vermont utilizzato dall'Agenzia non registra, in particolare, le interrogazioni effettuate dagli utenti attraverso Puntofisco e i *web service.*

Non risultano allo stato strumenti di controllo idonei a monitorare gli accessi effettuati attraverso l'applicativo *3270 enti esterni, web service e file transfer.*

Dagli atti emerge che gli amministratori locali degli enti esterni che accedono all'anagrafe tributaria non hanno effettuato i necessari controlli, anche periodici, sugli accessi e sulla sussistenza dei requisiti per le abilitazioni e le autorizzazioni degli utenti, anche per l'assenza di idonei strumenti a ciò finalizzati; tali soggetti, oltre alle anomalie relative alla gestione degli utenti riscontrate nei punti precedenti, non sono dotati di un sistema di *alert* o di un "cruscotto" che consenta loro di monitorare a livello statistico gli accessi all'anagrafe tributaria da parte degli utenti dell'ente. Peraltro, in taluni enti sono presenti più amministratori la cui attività non è risultata essere coordinata.

Prescrizioni

L'Agenzia deve predisporre idonee e concrete procedure di *audit* anche periodiche sugli enti esterni e anche sull'attività svolta da Sogei S.p.a. in qualità di responsabile del trattamento. In particolare, per quanto riguarda gli enti esterni, oltre ad attività di *audit* basate sul monitoraggio delle transazioni e su

sistemi di *alert*, tali procedure devono prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso.

Negli strumenti di *business intelligence* (applicativo Vermont o altri analoghi) utilizzati dall'Agenzia per monitorare gli accessi all'anagrafe tributaria dovranno confluire i *log* relativi a tutti gli attuali e futuri applicativi utilizzati per gli accessi da parte degli enti esterni.

Deve essere prefigurata da parte dell'Agenzia l'attivazione di specifici *alert* che individuino comportamenti anomali o a rischio, anche attraverso il monitoraggio e l'analisi periodica, a livello statistico, dei dati relativi alle transazioni eseguite dagli enti esterni.

Gli amministratori locali presso gli enti esterni devono essere dotati di strumenti di gestione delle utenze più efficaci e intuitivi che prevedano anche la possibilità di monitoraggi statistici degli accessi con l'attivazione di sistemi di *alert.* Gli strumenti in dotazione agli amministratori locali devono essere idonei a supportare i controlli che gli enti sono tenuti ad effettuare ai sensi delle convenzioni che autorizzano l'accesso all'anagrafe tributaria. Tali controlli devono riguardare in particolare, anche a campione, la rispondenza delle interrogazioni a una precisa finalità amministrativa (cfr. l'inserimento del numero di pratica nell'applicativo), e essere effettuati con cadenze periodiche e documentati con le modalità stabilite con l'Agenzia.

***

Le prescrizioni sopra illustrate devono essere predisposte al più presto. Anche sulla base del confronto con l'Agenzia -curato da ultimo dall'Ufficio- rispetto all'impiego delle risorse necessarie per la loro idonea attuazione e tenuto conto del rispetto dei diritti degli interessati, si ritiene necessario che le misure e gli accorgimenti sopra indicati, valutati singolarmente e nel loro complesso, siano accorpati in due distinti gruppi di adempimenti che dovranno essere posti in essere dall'Agenzia entro i termini, rispettivamente, di tre e di sei mesi. Limitatamente a taluni specifici e limitati profili, considerata la particolare complessità organizzativa richiesta, alcune delle misure e degli accorgimenti indicati devono essere invece completati entro il temine di dodici mesi. L'adempimento di tutte le prescrizioni del Garante dovrà essere, di volta in volta, puntualmente documentato a questa Autorità nei termini indicati decorrenti dalla data di ricezione del presente provvedimento.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive all'Agenzia delle entrate, con particolare riferimento alle attività dei soggetti esterni che accedono all'anagrafe tributaria, di adottare al più presto le misure e gli accorgimenti seguenti al fine di porre rimedio alle carenze indicate in motivazione, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati, rendendo il trattamento conforme alle disposizioni vigenti e provvedendo comunque entro, e non oltre, i distinti termini di volta in volta indicati. L'adempimento delle prescrizioni dovrà essere, di volta in volta, documentato puntualmente a questa Autorità nei medesimi termini indicati decorrenti dalla data di ricezione del presente provvedimento.

a) Con riferimento ai profili generali relativi agli accessi all'anagrafe tributaria da parte di soggetti esterni all'amministrazione finanziaria:

I) entro 6 mesi:

- l'Agenzia deve redigere con formalità descrittive *standard* un documento, costantemente aggiornato, che riporti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattivo, *batch* o di altro genere, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a realizzarlo, la base normativa, la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza e il volume dei trasferimenti o degli accessi e il numero di soggetti che utilizzano la procedura. Tale documento deve essere mantenuto costantemente aggiornato, e reso disponibile nel caso di controlli;
- con cadenza periodica annuale, l'Agenzia deve verificare l'attualità delle finalità per cui ha concesso l'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscere informazioni che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti;

II) entro 12 mesi:

- l'Agenzia deve introdurre nelle applicazioni volte all'uso interattivo da parte di incaricati un campo per l'indicazione obbligatoria del numero di riferimento della pratica nell'ambito della quale viene effettuata la consultazione;
- devono essere segmentati per quanto più possibile i dati visualizzabili attraverso gli applicativi (in modo cronologico, geografico e per tipologia di dati).

b) In relazione alla sicurezza dei sistemi di autenticazione degli applicativi utilizzati, l'Agenzia delle entrate deve:

I) entro 3 mesi:

- prevedere che tutte le applicazioni accessibili da rete pubblica in forma di *web application* siano implementate con protocolli *https/ssl* provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una *Certification Authority* ufficiale;
- permettere la visualizzazione, nella prima schermata successiva al collegamento, di 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 stesse informazioni devono essere riportate anche relativamente alla sessione corrente;
- disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali, limitandone l'utilizzo ai soli casi necessari per esigenze di servizio. In ogni caso, tale possibilità deve essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti. Nel caso in cui non sia possibile individuare la postazione di lavoro, la possibilità di accessi contemporanei deve essere inibita;

II) entro 6 mesi:

- provvedere all'implementazione di un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

c) Per quanto riguarda gli amministratori locali, le abilitazioni e le autorizzazioni degli utenti occorre che:

I) entro 3 mesi:

- nelle convenzioni che disciplinano l'accesso all'anagrafe tributaria sia previsto che gli enti esterni individuino gli "amministratori locali" sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Questi soggetti, prima di intraprendere la loro attività, devono essere formati dall'Agenzia delle entrate in ordine alle funzionalità dell'applicativo e all'attività di autorizzazione degli utenti. L'amministratore locale dell'ente esterno che accede all'anagrafe tributaria deve rimanere il punto di riferimento per le richieste di abilitazione e autorizzazione con la possibilità di gestire direttamente le utenze;
- l'Agenzia stabilisca nelle convenzioni che gli enti esterni debbano istruire adeguatamente il personale addetto all'utilizzo dei vari applicativi in ordine al corretto utilizzo delle funzionalità dei *software*. Le convenzioni, entro i medesimi termini, devono imporre agli enti, anche attraverso gli strumenti di *audit* in uso all'amministratore locale, controlli periodici i cui esiti devono essere documentati secondo le modalità definite nella stessa convenzione;
- le convenzioni stipulate dall'Agenzia predefiniscano una procedura per le autenticazioni e le autorizzazioni che coinvolga attivamente le figure apicali degli uffici interessati e un supervisore unico (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con l'amministratore tecnicamente deputato alla materiale gestione delle abilitazioni (e del relativo profilo), ma deve rispondere del controllo sullo stesso. Occorre inoltre che venga assicurato un flusso di comunicazione tra l'amministratore locale 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;
- in presenza di più amministratori locali per ciascun ente, l'Agenzia valuti e coordini i profili di autorizzazione da attribuire, garantendo in capo a un'unica figura la possibilità di intervenire su tutti gli utenti anche amministratori, monitorandone l'operato;
- l'Agenzia predefinisca, soglie relative al numero di utenti abilitabili da ciascun ente. Le richieste di superamento di tali soglie devono essere valutate caso per caso dall'Agenzia;
- siano previste limitazioni orarie per gli accessi, mantenendo comunque la possibilità di specifiche deroghe adeguatamente motivate;

II) entro 6 mesi:

- le *web application* predisposte dall'Agenzia per l'utilizzo da parte di enti esterni siano integrate, con procedure di "autenticazione forte" per ridurre la possibilità di usi impropri delle credenziali. Tali procedure devono essere prefigurate nei confronti di quelle classi di utenti cui corrispondano profili di autorizzazione che risultano più critici e, comunque, almeno per tutti i profili di autorizzazione corrispondenti alle funzioni di amministrazione locale;
- le convenzioni stipulate con ciascun ente prevedano espressamente i vincoli necessari ad assicurare un corretto trattamento dei dati e stabiliscano anche le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione.

d) Con riguardo ai singoli sistemi l'Agenzia deve:

I) entro 3 mesi:

- rispetto all'applicativo Siatel, introdurre misure di controllo per la funzionalità di "fornitura dati" visualizzabile nell'apposita schermata dell'applicativo e, con riferimento alle funzionalità utilizzabili da parte degli operatori comunali a soli fini anagrafici, inserire nell'applicativo medesimo specifiche indicazioni all'amministratore locale affinché vengano autorizzati solo utenti che agiscono presso l'ufficio anagrafe del comune;
- per quanto riguarda l'applicativo Puntofisco, aggiornare il profilo di autorizzazione assegnato agli enti esterni abilitati, escludendo a priori la consultabilità di dati sensibili laddove non sussista un'idonea base normativa. All'interno della procedura informatica di gestione degli utenti in uso all'amministratore locale devono essere inserite indicazioni che consentano all'Agenzia di visualizzare lo *status* di tutte le utenze con i profili abilitativi correnti, comprese quelle già cancellate. Entro il medesimo termine, deve essere corretta l'anomalia, relativa al sistema di gestione, che non permette regolarmente all'amministratore locale, visualizzando il profilo del singolo utente, di conoscerne l'effettiva possibilità di accesso dello stesso al sistema;
- per quanto riguarda gli applicativi Entratel e Fisconline/Cassetto fiscale, configurare i sistemi in modo da poter verificare il rispetto delle prescrizioni indicate nell'Allegato B al Codice relative, con particolare riferimento al sistema di scadenza delle *password* e all'attribuzione di credenziali idonee a identificare direttamente, oltre all'ente abilitato, anche il singolo incaricato che fisicamente effettua l'accesso, autentica e trasmette i file;

II) entro 6 mesi:

- realizzare la migrazione degli enti a oggi abilitati ad accedere all'anagrafe tributaria mediante 3270 enti esterni verso applicativi che offrono maggiori garanzie;
- con riferimento ai *web service*, effettuare una ricognizione dei servizi attualmente esposti e sospenderne l'attività in attesa della revisione delle attuali modalità di implementazione con le misure e gli accorgimenti di seguito descritti. Laddove l'Agenzia intenda impiegare *web service* esposti anche in rete pubblica per l'utilizzo da parte di enti esterni, questi devono essere configurati offrendo un livello minimo di accesso ai dati e limitando i risultati delle interrogazioni a valori di tipo *booleano*. Le convenzioni per l'utilizzo di tali servizi, inoltre, devono prevedere stringenti condizioni d'uso tali da consentire anche un'effettiva capacità di controllo da parte dell'Agenzia. Dal punto di vista tecnico, tali condizioni d'uso dei *web service* devono essere trasposte in appositi "accordi di servizio", redatti secondo il modello della cooperazione applicativa impiegata all'interno del sistema pubblico di connettività istituito dal Codice dell'amministrazione digitale. Gli "accordi di servizio" devono individuare idonee garanzie per il trattamento dei dati personali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con possibilità di identificazione dell'utente che accede ai dati, il *timestamp*, l'indirizzo Ip di provenienza dell'utente e del server interconnesso, l'operazione effettuata e i dati trattati;

III) entro 12 mesi:

- realizzare i collegamenti per la gestione di flussi di dati mediante *file transfer* su canali di connessione sicuri e garantire, anche attraverso la configurazione dei sistemi, che le credenziali di abilitazione utilizzate dagli operatori dell'ente esterno rispettino le prescrizioni indicate nell'Allegato B al Codice, in particolare identificando il soggetto che effettua lo scambio dei dati e prevedendo che la parola chiave prevista sia soggetta a scadenza periodica secondo i termini ivi indicati.

e) In relazione alle procedure di *audit* sull'accesso alle informazioni contenute nell'anagrafe tributaria da parte di soggetti esterni:

I) entro 3 mesi:

- l'Agenzia deve predisporre idonee e concrete procedure di *audit* anche periodiche sugli enti esterni e anche sull'attività svolta da Sogei S.p.a. In particolare, per quanto riguarda gli enti esterni, oltre ad attività di audit basate sul monitoraggio delle transazioni e su sistemi di *alert*, tali procedure devono prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso;

II) entro 6 mesi:

- negli strumenti di *business intelligence* utilizzati dall'Agenzia per monitorare gli accessi all'anagrafe tributaria devono confluire i *log* relativi a tutti gli attuali e futuri applicativi utilizzati per gli accessi da parte degli enti esterni;
- deve essere prefigurata da parte dell'Agenzia l'attivazione di specifici *alert* che individuino comportamenti anomali o a rischio, anche attraverso il monitoraggio e l'analisi periodica, a livello statistico, dei dati relativi alle transazioni eseguite dagli enti esterni;
- gli amministratori locali presso gli enti esterni devono essere dotati di strumenti di gestione delle utenze più efficaci e intuitivi che prevedano anche la possibilità di monitoraggi statistici degli accessi con l'attivazione di sistemi di *alert*. Gli strumenti in dotazione agli amministratori locali devono essere idonei a supportare i controlli che gli enti sono tenuti ad effettuare ai sensi delle convenzioni che autorizzano l'accesso all'anagrafe tributaria. Tali controlli devono riguardare, in particolare, anche a campione la rispondenza delle interrogazioni ad una precisa finalità amministrativa e essere effettuati con cadenze periodiche e documentati con le modalità stabilite con l'Agenzia.

Roma, 18 settembre 2008

IL PRESIDENTE
Pizzetti
IL RELATORE
Pizzetti
IL SEGRETARIO GENERALE
Buttarelli