Professionisti: obblighi antiriciclaggio, privacy e in qualità di intermediari

di Gianfranco Costa

Pubblicato il 3 Dicembre 2016

l'attività dei professionisti del settore fiscale è soggetta a onerosi compiti amministrativi per il rispetto delle normative su privacy e antiriciclaggio; in questo articolo di 16 pagine analizziamo quali sono gli adempimenti per gli intermediari del Fisco per la corretta costruzione del fascicolo del cliente nel rispetto della privacy e dell'antiriciclaggio

Negli ultimi anni l'Amministrazione Finanziaria ha effettuato dei controlli sui professionisti volti a verificare il rispetto degli adempimenti previsti a loro carico dalle norme sull'invio delle dichiarazioni e sul rispetto delle previsioni a tutela della privacy.

Al fine di identificare meglio l'attività promossa dai verificatori, analizziamo le previsioni normative.

L'attività di intermediario fiscale

Il dato normativo è contenuto nel D.P.R. n. 322/1998 il quale contiene le previsioni sui soggetti titolati a svolgere l'attività di intermediario fiscale e delle modalità e termini per l'invio delle dichiarazioni.

Soggetti titolati ad inviare all'Amministrazione Finanziaria le dichiarazioni, ai sensi dell'articolo 3, comma 3 del citato Decreto, sono:

- gli iscritti negli Albi dei Dottori Commercialisti, dei Ragionieri e dei Periti Commerciali e dei Consulenti del Lavoro;

- iscritti alla data del 30.09.1993 nei ruoli dei periti ed esperti presso le Camere di Commercio in possesso di laurea in giurisprudenza, in economia e commercio o equipollenti o i ragionieri;

- coloro che esercitano abitualmente l'attività di consulenza fiscale (D.M. 19.04.2001);
- le associazioni sindacali di categoria tra imprenditori, nonché quelle che associano soggetti appartenenti a minoranze etnico-linguistiche;
- i Centri di Assistenza Fiscale per le imprese e per i lavoratori dipendenti e pensionati.

Per poter colloquiare con l'Amministrazione finanziaria, l'intermediario deve prima di tutto richiedere l'abilitazione presso l'Agenzia delle Entrate territorialmente competente.

A questo punto:

- il contribuente, che intende servirsi dell'intermediario, deve presentare la dichiarazione in tempo utile per consentigli il rispetto dei termini;
- l'intermediario può accettare o rifiutare l'incarico di trasmissione della dichiarazione predisposta dal contribuente.

Ricordiamo che l'intermediario è obbligato all'invio telematico delle dichiarazioni:

- da lui predisposte;
- sulle quali ha apposto il visto di conformità sui crediti (C.M. n. 57/E/2009);
- delle quali ha accettato l'incarico di trasmissione (impegno a trasmettere).

Stabilito che l'intermediario si è assunto l'onere di inviare le dichiarazioni del proprio cliente è importante ricordare che:

- le eventuali variazioni dei dati anagrafici intercorse nel periodo compreso tra la presentazione della dichiarazione all'intermediario e la sua trasmissione telematica, non obbligano l'intermediario a modificare la dichiarazione presentata;
- le dichiarazioni presentate all'intermediario dopo la scadenza del termine di presentazione (esempio 30.09) devono essere trasmesse entro 30 giorni dalla data dell'impegno a trasmettere;

- la dichiarazione deve essere firmata dal contribuente, ma la mancata sottoscrizione può essere sanata entro 30 giorni dall'invito dell'Agenzia.

Va ricordato che la dichiarazione si considera presentata nel giorno in cui è trasmessa. La prova di presentazione è data dalla comunicazione di avvenuto ricevimento rilasciata dall'Agenzia delle Entrate.

Importante rammentare che per le dichiarazioni predisposte dal contribuente, l'intermediario rilascia al contribuente l'impegno a trasmettere in via telematica i dati contenuti nella dichiarazione, ma non ha responsabilità sui contenuti.

Effettuata la trasmissione telematica, entro 30 giorni dal termine per l'invio telematico l'intermediario rilascia al contribuente:

- un originale della dichiarazione trasmessa e sottoscritta dall'intermediario;
- copia della ricevuta di presentazione.

È sempre importante ricordare che l'intermediario deve essere in condizione di dimostrare ai verificatori che ha adempiuto ai vari obblighi. Quindi è utile avere una ricevuta o una dichiarazione di consegna della dichiarazione spedita e della ricevuta di Entratel.

Rammentiamo poi che l'impegno a trasmettere la dichiarazione rilasciato dall'intermediario non esclude dalla responsabilità il contribuente in caso di mancata presentazione (C.M. 25.01.2002, n. 6/E). Su questo tema c'è una sentenza della Suprema Corte di Cassazione (ordinanza 01.06.2012, n. 8805) che sostiene la non imputabilità al contribuente dell'omesso invio di una dichiarazione quando il contribuente è in possesso dell'impegno alla trasmissione, ma per il momento è una presa di posizione giurisprudenziale isolata, seppur autorevole.

Per continuare sugli adempimenti ricordiamo che gli intermediari sono tenuti a conservare anche su supporti informatici, per il periodo prescrizionale di accertamento (4° periodo d'imposta successivo al termine di presentazione della dichiarazione – salvo le situazioni dei soggetti che non hanno aderito al condono), copia delle dichiarazioni trasmesse (R.M. 18.10.2007, n. 298).

Dal 2008, le comunicazioni di irregolarità, possono essere inviate dall'Agenzia delle Entrate direttamente all'intermediario, se vi è stata apposita opzione nella dichiarazione. L'intermediario che ha accettato tale

compito entro 60 giorni dal ricevimento della notifica le dovrà notificare al contribuente. Eventualmente dovrà comunicare all'Agenzia delle Entrate che il contribuente non è più cliente dell'intermediario.

Adempimenti Privacy

Dal momento che le verifiche promosse dall'Agenzia delle Entrate si estendono anche agli adempimenti inerenti la privacy, vediamo di fare una breve trattazione anche di questa materia.

Partiamo, prima di tutto con una analisi delle definizioni contenute nell'articolo 4 del D.lgs. n. 196/2003.

Trattamento" qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti:

- la raccolta;
- la registrazione;
- l'organizzazione;
- la conservazione;
- la consultazione;
- l'elaborazione, la modificazione;
- la selezione, l'estrazione, il raffronto;
- l'utilizzo, l'interconnessione, la comunicazione, la diffusione;
- la cancellazione e la distruzione di dati;

anche se non registrati in una banca dati.

Dato personale: qualunque informazione:

- relativa a persona fisica o giuridica, Ente o associazione;

- identificati o identificabili;
- anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati sensibili: i dati personali idonei a rivelare:

- l'origine razziale ed etnica;
- le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche;
- l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale;
- nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Titolare del trattamento:

la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile del trattamento:

la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, associazione od organismo preposti dal “titolare del trattamento” al trattamento di dati personali.

Incaricati al trattamento: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile sono nominati incaricati tutti coloro che raccolgono, elaborano e utilizzano dati personali, siano essi lavoratori dipendenti o autonomi e collaboratori esterni. La nomina deve avvenire per scritto e contiene indicazioni precise dell’ambito del trattamento consentito.

Interessato:

la persona fisica, la persona giuridica, l'Ente o l'associazione cui si riferiscono i dati personali.

Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell’articolo 31.

“Articolo 31. Obblighi di sicurezza. 1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta”.

Con il Provvedimento n. 1577499 del 27.11.2008 viene introdotta una nuova figura: l’amministratore di sistema.

Con la definizione di “amministratore di sistema” si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente Provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati:

- quali gli amministratori di basi di dati;
- gli amministratori di reti e di apparati di sicurezza;
- e gli amministratori di sistemi software complessi.

Informativa all’interessato: generalmente è un atto che rende noto all’interessato:

- chi tratta i dati;
- le modalità del trattamento;
- e i diritti riconosciuti dalla legge.

Deve essere preventiva al trattamento e può essere data all’interessato:

- sia in forma orale (valutare la convenienza di questa scelta data la quasi nullità della capacità probatoria);
- che scritta.

Secondo quanto stabilito dall’articolo 13, l’informativa deve indicare:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto a rispondere;
- i soggetti ai quali i dati personali possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- i diritti dell'interessato, descritti nell'articolo 7 della Legge n. 196/03;
- gli estremi identificativi del titolare ed eventualmente del responsabile.

In caso di più responsabili indicarne almeno uno di essi.

Il trattamento di dati da parte di privati o Enti pubblici economici è ammesso solo con il consenso dell'interessato. Il consenso può riguardare l'intero trattamento o solo alcune operazioni. Il consenso è validamente espresso:

- se è documentato per scritto;
- e se l'interessato ha avuto le informazioni dell'articolo 13.

Il consenso deve essere in forma scritta se riguarda dati sensibili.

Il consenso non è obbligatorio se il trattamento:

- è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato;
- riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, nei limiti previsti dalle norme;
- riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto delle norme in materia di segreto aziendale e industriale;

- è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo;
- è necessario ai fini dello svolgimento delle investigazioni difensive;
- è effettuato da associazioni, Enti o organismi senza scopo di lucro, in riferimento a soggetti che hanno con essi contratti regolari o ad aderenti, per il conseguimento degli scopi istituzionali;
- è necessario per esclusivi scopi scientifici, statistici o per scopi storici presso archivi privati dichiarati di notevole interesse;
- viene effettuato per ragioni di giustizia, informatica giuridica, polizia, difesa e sicurezza dello Stato e altre finalità di interesse pubblico.

Il D.L. n. 70/2011 ha apportato alcune modifiche alle disposizioni sulla privacy.

Le comunicazioni relative alla riservatezza dei dati personali sono limitate alla tutela dei cittadini. Pertanto, il trattamento dei dati personali relativi a persone giuridiche, imprese, Enti o associazioni effettuato nell'ambito di rapporti intercorrenti esclusivamente tra i medesimi soggetti per finalità amministrativo-contabili è esonerato dall'applicazione delle disposizioni del D.lgs. n. 196/2003.

Il trattamento dei dati contenuti nei curriculum trasmessi spontaneamente alle imprese non richiede il consenso dell'interessato al momento del primo contatto successivo all'invio dei curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, un'informativa breve sul trattamento dei dati.

Il DPS è sostituito da un'autocertificazione:

- per le imprese che trattano solo dati personali non sensibili;
- ovvero come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli del coniuge e dei parenti.

L'autocertificazione è resa dal titolare del trattamento attesta di trattare solo tali dati in osservanza delle misure minime di sicurezza.

Tecniche di protezione dei dati

Per la tutela degli archivi elettronici, negli stessi devono essere inserite chiavi o password.

Le chiavi possono essere contenute in appositi dispositivi magnetici o digitate all'apertura dell'archivio.

Le chiavi devono essere conosciute:

- dall'operatore;
- e dal responsabile del trattamento.

Le chiavi devono essere periodicamente modificate per garantire la riservatezza.

La parola chiave o password, come riportato dall'articolo 4 del Codice:

- è associata ad una persona e ad essa nota;
- è costituita da una sequenza di caratteri (alfabetici, numerici, simbolici) o altri dati in forma elettronica:
- • • può contenere cioè tutti i segni riportati sulla tastiera e usati con libertà di scelta e combinazione.

La sua lunghezza, dove il sistema lo permetta, non dovrà mai essere inferiore a 8 caratteri. Se il sistema non lo permette, il numero dei caratteri dovrà essere pari al massimo consentito da tale sistema. Inoltre, deve essere aumentata in proporzione all'importanza e alla natura dei dati trattati.

La password:

- è negata la possibilità di utilizzare parole facilmente individuabili quali il proprio nome o quello di un familiare;
- non deve essere associata a nulla di logico che sia interpretabile o riconoscibile da qualsiasi persona in quanto riferita a caratteristiche note del suo titolare;
- evitare ripetizioni consecutive di caratteri;
- scegliere, dove possibile, l'uso di maiuscole e minuscole, lettere, numeri ed altri caratteri;

- usarla in modo che non venga mai scritta e annotata in luoghi facilmente visibili ad altri;
- non appaia sul video quando viene digitata;
- non venga digitata davanti ad altre persone;
- non risulti visibile attraverso le varie funzioni di stampa.

La durata di una password, ai sensi del punto 5 del Disciplinare, non può essere superiore a:

- 6 mesi, decorsi i quali dovrà essere modificata;
- 3 mesi, per i trattamenti di dati sensibili e giudiziari, in quanto richiedono protezioni maggiori.

È fondamentale ricordare, il terminale non può essere lasciato incustodito dall'operatore è consigliato impostare il terminale in modo che si attivi lo screen saver e che alla sua riattivazione venga richiesta la password.

Per quanto riguarda l'antivirus ed il sistema operativo, sarà necessario:

- installare ed aggiornare di frequente i programmi antivirus;
- installare periodicamente gli ultimi aggiornamenti del sistema operativo e delle applicazioni.

Il Disciplinare Tecnico, al punto 16, parla di cadenza almeno semestrale per:

- l'aggiornamento degli antivirus;
- l'aggiornamento dei sistemi operativi.

L'utilizzo di supporti quali floppy disk, cd-rom o nastri che contengono dati sensibili o giudiziari (punto 22 del Disciplinare Tecnico) se contengono dati sensibili o giudiziari non utilizzati devono essere distrutti o resi inutilizzabili.

Per essere riutilizzati le informazioni in essi contenute non devono essere intelligibili e tecnicamente in alcun modo ricostruibili.

Questi obblighi sono volti, naturalmente, ad evitare che i dati contenuti nei supporti siano conosciuti, anche accidentalmente, da soggetti che non sono autorizzati a farlo.

Ai sensi dell'articolo 34, comma 1, lettera f, punti 18 e 23 del Disciplinare Tecnico, per la tutela dei dati è necessario realizzare una copia degli archivi.

Il titolare decide le modalità per effettuare le copie, il contenuto, la frequenza e la custodia in luoghi sicuri, accessibili solo agli incaricati, delle copie stesse per garantire in tempi brevi il ripristino dei dati, ma va ricordato che il ripristino dei dati in presenza di dati sensibili o giudiziari deve avvenire in massimo sette giorni.

Il disciplinare tecnico al punto 18 prevede che il salvataggio degli archivi avvenga settimanalmente. Il ripristino dei dati, utilizzando le più recenti copie di sicurezza, consente di riprendere l'attività e quindi anche il trattamento dei dati, garantendo i servizi offerti.

Il Documento Programmatico sulla Sicurezza – DPS

Il documento è una rappresentazione attenta e responsabile dei rischi aziendali e delle contromisure da adottare.

Esso ha un ruolo rilevante nella pianificazione delle scelte di sicurezza ed è una delle documentazioni obbligatorie che le imprese devono tenere, ove richiesto.

La scadenza originaria del 30 giungo è stata prima prorogata al 31 dicembre 2004 con il D.L. n. 158 del 24.06.2004 e poi al 30 giugno 2005 con il D.L. n. 266 del 09.11.2004.

Infine, con il D.L. n. 314 del 30.12.2004 è stata nuovamente prorogata al 31.12.2005.

Ogni anno, entro il 31 marzo, andava aggiornato.

Per la sua redazione era necessario effettuare le seguenti analisi preventive:

- analisi generale di tutti i trattamenti di dati personali svolti in azienda o affidati a terzi;

- esaminare ed elencare le disposizioni interne alla struttura e le responsabilità previste per il trattamento dei dati personali, in particolare:
- i dati trattati con strumenti elettronici;
- i dati sensibili e giudiziari trattati con i medesimi strumenti;
- la gestione organizzativa delle aree dove vengono svolti questi trattamenti;
- ampia ed accurata analisi dei rischi e delle circostanze che possano generare perdite, distruzioni, accessi non autorizzati, trattamenti non consentiti, ecc. dei dati. L'analisi deve tenere conto anche della natura dei dati, distinguendo fra quelli comuni, quelli sensibili e giudiziari, quelli che rilevano lo stato di salute e quelli genetici.

Il Documento Programmatico sulla Sicurezza doveva contenere:

- elenco dei trattamenti di dati personali;
- distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- analisi dei rischi che incombono sui dati;
- indicazioni per assicurare l'integrità e la disponibilità dei dati e le protezioni degli ambienti;
- misure da adottare per fare fronte ai rischi di distruzione e perdita dei dati;
- le indicazioni per il ripristino della disponibilità dei dati stessi;
- la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accesso;
- procedure e accorgimenti per:
- la generazione delle copie di sicurezza;
- la loro custodia;

- il loro funzionamento in caso di ripristino;

- descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare, in conformità al codice;

- evidenziare, ai fini della protezione dei dati, l'attività di formazione data agli incaricati del trattamento.

Va ricordato che nel casso di cessazione del trattamento dei dati, essi potranno essere:

- distrutti;

- ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;

- conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;

- conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

Semplificazioni

L'articolo 29 del D.L. n. 112/2008 individua una semplificazione con la sostituzione del DPS con un'autocertificazione e recita:

> *"Per i soggetti che trattano dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero all'adesione ad organizzazioni sindacali o a carattere sindacale, la tenuta di un aggiornato Documento Programmatico sulla Sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 … D.P.R. n. 445/2000, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per*

> *correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti, artigiani, il Garante, sentito il Ministro per la Semplificazione Normativa, individua con proprio Provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'allegato B) in ordine all'adozione delle misure minime …".*

Amministratore di sistema

Una se ne toglie ed una si inventa. Infatti, con il Provvedimento n. 1577499 del 27.11.2008, il Garante alla privacy ha introdotto l'amministratore di sistema. Vediamo l'incipit normativo:

"4. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici

- Di seguito sono indicati gli accorgimenti e le misure che vengono prescritti ai sensi dell'articolo 154, comma 1, lettera c) del Codice, a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici, esclusi, allo stato, quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione (articolo 29, D.L. 25 giugno 2008, n. 112, convertito, con modificazioni, con Legge 6 agosto 2008, n. 133; articolo 34 del Codice; Provvedimento Garante 6 novembre 2008).

4.3. Elenco degli amministratori di sistema

- Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

- Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti.

Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'articolo 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (ad esempio, intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità

non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

- Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema".

Privacy: sistema sanzionatorio

Dal punto di vista sanzionatorio, il mancato rispetto delle norme sulla privacy comporta un duplice sistema punitivo: uno amministrativo ed uno di carattere penale.

Sanzioni amministrative (articoli dal 161 al 168). Inerenti l'informativa:

- omessa o inidonea informativa all'interessato (articolo 161): da euro 6.000 a euro 36.000. La sanzione può essere quadruplicate se risulta inefficace per la situazione economica del contravventore.

Altre sanzioni:

- trattamento dei dati personali senza adottare le misure minime di sicurezza: da euro 10.000 a euro 120.000;
- cessione dei dati: da euro 10.000 a euro 60.000;
- comunicazione di dati sanitari effettuati da un medico non designato o da soggetto diverso dal titolare dei dati: da euro 1.000 a euro 6.000;
- mancata esibizione di documenti richiesti dal Garante: da euro 10.000 a euro 60.000.

Sanzioni penali (articolo 169):

- mancata adozione delle misure minime:
- • • arresto fino a due anni;

oppure

- ammenda euro 30.000, se si eseguono le prescrizioni del Garante.

Il Garante, in presenza di situazioni di particolare difficoltà a realizzare le misure minime, può concedere un termine entro cui regolarizzare la posizione. Il termine può essere prorogato ma non oltre 6 mesi. Nei 60 giorni successivi alla scadenza del termine, se si sono adempiuti gli obblighi, pagando un quarto del massimo della sanzione, il titolare sana la situazione ed estinguere il reato;

- mancato rispetto delle prescrizioni del Garante (articolo 170): arresto da 3 mesi a 2 anni;
- utilizzo di dati personali per trarre profitti personali (articolo 167): arresto da 6 a 18 mesi;
- comunicazione dei dati a terzi o loro diffusione: arresto da 6 a 24 mesi;
- notifica al Garante contenenti le false notizie: reclusione da 6 mesi a 3 anni.

Verifiche sugli intermediari

Analizzate le previsioni normative, passiamo ora alla fase dei controlli, percorrendo, nello specifico il contenuto del Comunicato Stampa 03.08.2011 a mezzo del quale l'Auditing dell'Agenzia delle Entrate ha fornito le istruzioni (poi implementate con informative interne all'Amministrazione) con le quali individua ciò che sarà oggetto di controllo.

Preliminarmente va detto che l'attività di controllo sugli adempimenti degli intermediari è svolta dalla Direzione Regionale delle Entrate competenze per il domicilio del verificato.

In secondo luogo va poi fatto notare che non si è di fronte ai tradizionali controlli nei quali i verificatori "piombano" in studio ed iniziano la verifica. In questo caso, arriva una comunicazione nella quale è fissato il giorno e l'ora di inizio della verifica.

Con apposita istanza la data può essere cambiata, tenendo conto comunque che lo slittamento potrà essere di pochi giorni.

Le Direzioni Regionali (Ufficio Audit Esterno) vigilano sull'intermediario nella fase di:

- autorizzazione allo svolgimento dell'attività (articolo 2, comma 4, D.P.R. n. 322 del 22.07.1998);
- verifica della regolarità della trasmissione (articolo 3, comma 8, D.P.R. n. 322 del 22.07.1998);
- verifica del rispetto della privacy (articolo 8, comma 1, lettera h) e articolo 11, comma 3, D.D. 31.07.1999).

Ha il compito di accertare che gli intermediari siano:

- efficienti nella loro attività;
- affidabili nei rapporti con l'Agenzia ed i contribuenti;
- preparati professionalmente;
- rispettosi della normativa privacy.

Per quanto riguarda i criteri utilizzati per la formazione delle liste di verifica, l'Auditing rileva:

- l'elenco dichiarazioni segnalate dall'applicativo MAIA come tardive / omesse (incrocio date impegno telematico con data di trasmissione e data di scadenza);
- elenco dichiarazioni segnalate dall'applicativo MAIA come presunte omissioni (incrocio dati depositario scritture contabili con dichiarazioni trasmesse);
- elenco intermediari con alte percentuali di anomalia.

Nota Bene: le tardività rilevano solo se risultano superiori:

- a 5 dichiarazioni fuori termine, valore indipendente dal periodo di presentazione;
- e 3 omissioni nell'invio di dichiarazioni.

Il comunicato stampa 03.08.2011 ha, di fatto, attivato le verifiche sul rispetto delle disposizioni sull'invio delle dichiarazioni e sugli adempimenti in tema di privacy. Queste verifiche sono effettuate dalla Direzione Regionale delle Entrate.

Le operazioni di verifica saranno volte a controllare che gli intermediari abbiano adottato le cautele necessarie a proteggere i dati personali e sensibili di cui vengono a conoscenza ai fini dello svolgimento della propria attività secondo quanto previsto dall'articolo 11 del Decreto 31.07.1998 e dall'articolo 5 del Provvedimento del Direttore dell'Agenzia delle Entrate del 10.06.2009.

La finalità dei controlli è la verifica dell'effettiva adozione di tutte le cautele necessarie a proteggere I dati personali e sensibili.

Per quanto riguarda i settori di intervento durante la fase di controllo, essi riguarderanno:

- la struttura organizzativa dell'intermediario;
- le misure di sicurezza relative ai supporti tecnologici utilizzati;
- le ulteriori misure di sicurezza.

Analizziamo ora nel dettaglio il contenuto del Comunicato Stampa, secondo i singoli settori di controlli appena descritti.

1. Struttura organizzativa dell'intermediario

Saranno oggetto di riscontro:

- l'eventuale designazione dei responsabili del trattamento dei dati;
- la redazione di istruzioni operative riservate agli stessi responsabili;
- l'esistenza del Documento Programmatico per la Sicurezza;
- la designazione degli incaricati per il trattamento dei dati e l'attribuzione dell'ambito di trattamento consentito;
- la sensibilizzazione dei soggetti che trattano i dati personali dei contribuenti circa le responsabilità connesse alla condivisione o comunicazione a persone non legittimate dei predetti dati acquisiti nello svolgimento delle proprie funzioni;

- l'adozione di una procedura di controllo del rispetto delle misure di sicurezza e dell'adempimento degli obblighi previsti dal D.lgs. n. 196/2003;
- l'adozione di una corretta politica di gestione delle password, che preveda:
- - - l'attribuzione a uno o più soggetti specifici dell'incarico di amministrare le utenze per l'accesso ai sistemi informatici;
    - l'utilizzo di credenziali di accesso nominative e note solo all'utente responsabile della loro conservazione;
    - l'indicazione da parte dell'intermediario ai propri collaboratori dei criteri che le password utilizzate devono rispettare;
- la previsione, nel ciclo di vita delle credenziali, di procedure per garantire la costante aderenza tra i privilegi di accesso ai dati e il ruolo organizzativo del personale che vi accede;
- la designazione, come responsabili del trattamento, delle società esterne diverse dalle società di servizi di cui l'intermediario si avvalga per operazioni meramente strumentali all'esercizio dell'assistenza fiscale (esempio: ripristino di un server o la sostituzione di un supporto hardware).

2. Misure di sicurezza relative ai supporti tecnologici utilizzati

Sarà verificata l'adozione di misure di protezione delle postazioni di lavoro, dei server e dell'infrastruttura di rete. In particolare, sarà riscontrata la sussistenza di:

- configurazione delle stazioni di lavoro che preveda il blocco automatico delle stesse dopo un certo tempo di inattività dell'operatore;
- installazione di programmi di protezione per le stazioni di lavoro e server;
- aggiornamento periodico del sistema operativo e del software di protezione;
- in caso di utilizzo di reti senza fili (wireless), adozione di protocolli di sicurezza idonei a limitare il rischio che le trasmissioni dati siano intercettabili da parte di soggetti esterni non autorizzati.

3. Ulteriori misure di sicurezza

Sarà verificata l'adozione delle seguenti misure di sicurezza:

- conservazione delle dichiarazioni e della relativa documentazione separatamente dai documenti acquisiti dall'intermediario per altre attività dallo stesso svolte:
- un armadio per la contabilità;
- un armadio per le dichiarazioni;
- conservazione separata dei documenti contenenti dati sensibili dal resto della documentazione archiviata:
- spese mediche, opzioni 8‰, ecc., in busta chiusa;
- presenza di spazi idonei ed accessibili esclusivamente a personale autorizzato per la conservazione dei documenti relativi all'attività di trasmissione delle dichiarazioni fiscali e dei supporti contenenti il backup dei dati stessi:
- esistenza, nei casi in cui l'attività di assistenza / trasmissione non si risolva in un'opera pressoché personale del soggetto abilitato, ma si dispieghi, piuttosto, in base ad un'articolata struttura organizzativa, di procedure per l'accesso e la gestione degli archivi;
- conservazione della documentazione fiscale secondo le modalità e per il periodo previsti dalle vigenti disposizioni

Esito dei controlli

Secondo quanto previsto dall'articolo 8 del D.M. 31.07.1998, il mancato rispetto dei predetti obblighi di riservatezza costituisce causa di revoca dell'abilitazione al canale Entratel.

Le irregolarità emerse dai controlli saranno segnalate, quindi, dagli Uffici di audit alle strutture delle Direzioni regionali.

19 settembre 2016

Gianfranco Costa