Allegato 4

Raccomandazioni agli operatori finanziari formulate dal

Garante per la protezione dei dati personali

Gli operatori finanziari devono assicurare che:

a) i soggetti che intervengono nelle procedure di estrazione e invio siano scelti dagli operatori finanziari sulla base di elevati requisiti di idoneità soggettiva in termini di affidabilità e competenze, preferibilmente tra coloro che abbiano un rapporto stabile con essi;

b) anche in considerazione delle dimensioni dell'operatore finanziario, siano adottati meccanismi di cifratura e di sicurezza, rispettivamente finalizzati a proteggere le informazioni contenute nel *file* durante i successivi passaggi all'interno dell'operatore stesso e ad assicurare l'integrità del contenuto e a prevenirne alterazioni;

c) l'accesso al *file*, nelle successive fasi del trattamento, anche dopo la cifratura, sia circoscritto ad un numero il più possibile limitato di incaricati;

d) qualora la comunicazione all'Agenzia delle Entrate avvenga mediante l'utilizzo di caselle di PEC alimentate in modo non completamente automatico, e quindi attraverso postazioni client, tali postazioni devono disporre, come da ordinarie prassi di sicurezza informatica, di versioni costantemente aggiornate del sistema operativo, del browser, dei programmi antivirus e degli altri software applicativi utilizzati sulla postazione medesima, al fine di ridurre i rischi connessi ad accessi non consentiti o all'azione di virus o altri *malware*;

e) qualora gli operatori finanziari decidano di affidare la comunicazione a soggetti esterni, designati responsabili o incaricati del trattamento, il *file* sia loro fornito già cifrato;

f) il *file* cifrato che viene trasmesso ai predetti soggetti esterni per la successiva trasmissione all'anagrafe tributaria sia conservato sui nodi di interscambio per il tempo strettamente necessario allo scambio dei dati. L'operatore finanziario deve verificare l'avvenuta cancellazione dai nodi di interscambio subito dopo la ricezione delle relative ricevute;

g) anche le comunicazioni a mezzo PEC contenenti dati personali, ancorché cifrati, siano cancellate da parte dell'operatore dai server di posta utilizzati per la comunicazione, una volta completata la procedura di invio o ricezione;

h) gli operatori finanziari, soggetti in capo ai quali sono demandate la gestione delle utenze e delle credenziali di autenticazione FTP, rispettino le misure minime di sicurezza di cui all'Allegato B del Codice, comunicando all'Agenzia periodicamente con scadenza prefissata su canali sicuri la nuove credenziali di autenticazione per l'accesso ai propri server FTP;

i) i nodi di interscambio devono disporre di uno spazio FTP dedicato alla comunicazione integrativa annuale; in caso di nodi che servono più operatori finanziari, tale spazio deve essere distinto per ciascuno di essi; anche le credenziali di accesso al server FTP devono essere riferite unicamente alla comunicazione integrativa annuale di ogni singolo operatore;

1) con riferimento al ruolo assunto dai nodi di interscambio rispetto al trattamento dei dati personali, ancorché cifrati, qualora l'invio avvenga per conto terzi:

- tale soggetto sia preventivamente designato quale responsabile del trattamento il gestore del nodo, che deve offrire idonee garanzie in relazione a quanto previsto dall'art. 29 del Codice;
- siano fornite a tale soggetto adeguate istruzioni e vigili sul trattamento da effettuare, con particolare riguardo alle ipotesi in cui tale soggetto sia designato responsabile da più operatori, al fine di garantire misure di carattere tecnico organizzativo volte ad assicurare la segregazione dei flussi tra l'Agenzia e ciascun operatore;

m) riguardo alla possibilità di avvalersi di nodi di interscambio già certificati o consorziati, e quindi esterni, sia garantito che la trasmissione al nodo del *file* da comunicare all'anagrafe tributaria avvenga con misure di sicurezza analoghe a quelle assicurate nell'interscambio tra il nodo medesimo a l'Agenzia delle Entrate.