Ordine dei
Dottori Commercialisti
e degli Esperti Contabili
di Ivrea, Pinerolo, Torino

Le procedure organizzative dell'intermediario per garantire la riservatezza

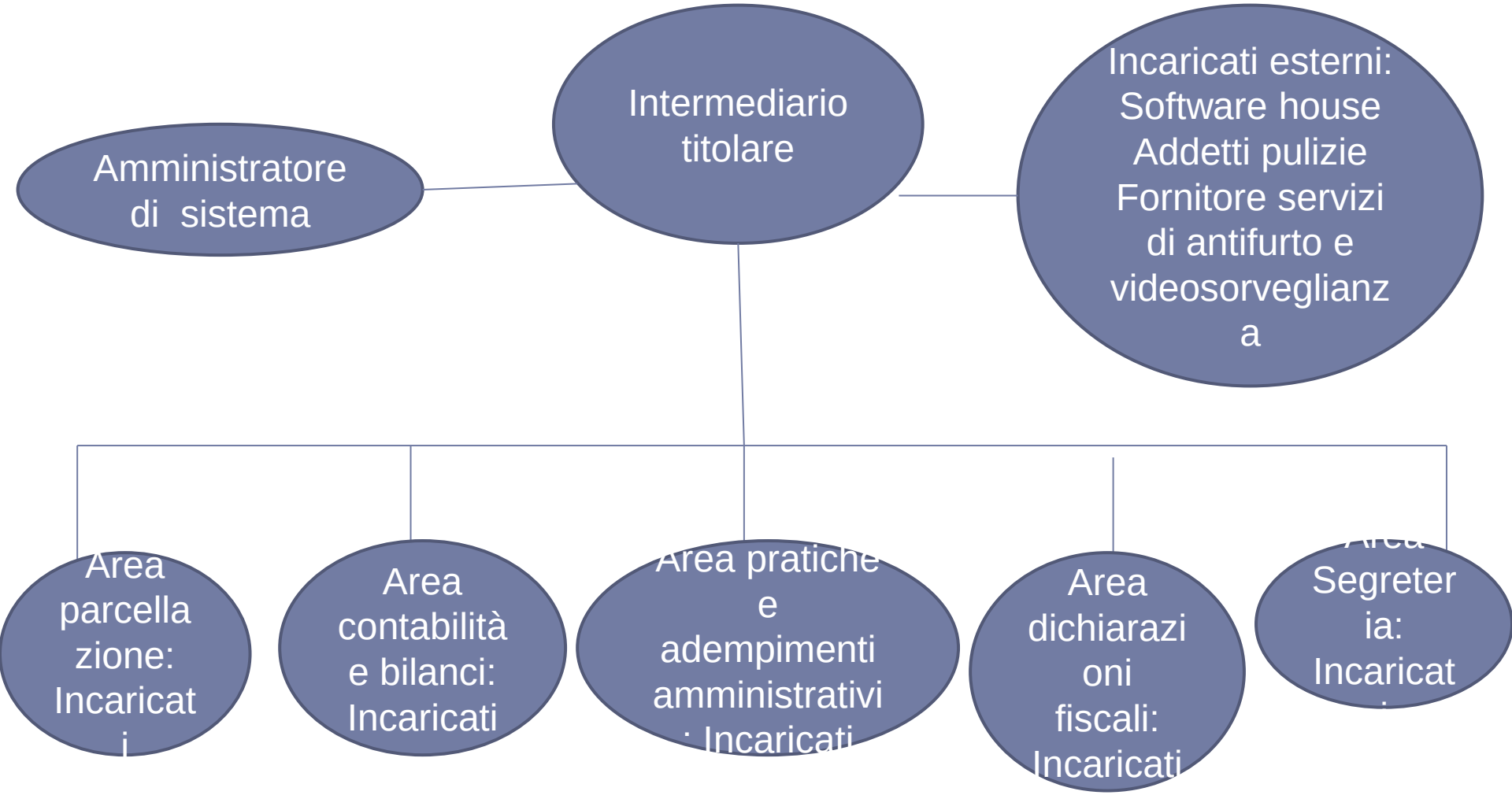
Torino 22/03/2013 – dott. Giuseppe Scolaro

Gli adempimenti privacy nell'attività dell'intermediario Entratel: L'informativa

- Ai fini del rispetto degli adempimenti fissati dall'art. 11 del D.M 31/07/1998, del Ministero delle Finanze - Agenzia delle Entrate, il professionista è tenuto al rispetto delle disposizioni previste dal d.lgs. 30/06/2003 n. 196 In particolare:
  - Dare prova della corretta informativa ai sensi dell'art. 13 del d.lgs. n. 196/2003, nella quale sia data evidenza della finalità del trattamento, si evinca che siano state date le informazioni con riguardo al titolare del trattamento, all'eventuale responsabile del trattamento, ove nominato, luogo in cui è effettuato il trattamento, modalità del trattamento dei dati, indicazione dei recapiti anche elettronici a cui il soggetto può rivolgere le proprie comunicazioni ai fini dell'esercizio della tutela personale, le finalità del trattamento dei dati, e infine i soggetti a cui potranno essere comunicati i dati. Per effetto delle semplificazioni introdotte dal D. Lgs. del 9 febbraio 2012 n. 5 (art. 45)
    - E' possibile fornire un'unica informativa per il complesso dei trattamenti anziché per i singoli aspetti del rapporto con il soggetto interessato.
  - Dare prova dell'acquisizione del consenso per il trattamento dei dati sensibili (scelta per l'attribuzione dell'otto per mille e del 5 per mille, trattamento dei dati relativi allo stato di salute e/o l'iscrizione a sindacati).
    - Nessun consenso è da raccogliere quando il trattamento dei dati è svolto, anche in relazione all'adempimento di obblighi contrattuali, precontrattuali o normativi, esclusivamente per normali finalità amministrative e contabili, nonché quando i dati provengono da pubblici registri ed elenchi pubblici conoscibili da chiunque, o sono relativi allo svolgimento di attività economiche o sono trattati da un soggetto pubblico.
- La prova dell'adeguata informativa ottempera agli obblighi indicati ai commi 1, 2 e 3 dell'art. 11 del citato D.M. 31/07/1998.

Gli adempimenti privacy nell'attività dell'intermediario Entratel: l'organigramma

- L'attività di controllo è volta a verificare la struttura dell'organizzazione dell'intermediario, pertanto è bene che la struttura predisponga ed aggiorni un organigramma in grado di rappresentare le figure richieste dalla normativa e le aree funzionali dello studio con riguardo alle attività dei soggetti:
  - Titolare del trattamento
  - Eventuale responsabile del trattamento
  - Aree funzionali dello studio con evidenza dei soggetti incaricati
  - Amministratore di sistema per la gestione dei sistemi informatici
  - Incaricati esterni per la manutenzione dei sistemi informatici, per le pulizie dei locali, per interventi di manutenzione alla struttura.
- L'eventuale nomina da parte del titolare (intermediario Entratel) di un responsabile e la nomina degli incaricati interni al trattamento dei dati ed esterni ottempera per interventi sugli strumenti elettronici con cui è effettuato il trattamento, deve essere provato, La nomina del responsabile del trattamento è facoltativa ai sensi dell'art. 29 del d.lgs 196/2003 ed in caso di nomina ottempera alla disposizione dell'art. 11, comma 3 del D.M. 31/07/1998 e dell'art. 5,, comma 4 del provvedimento 10/06/2009.


Amministratore di sistema
Intermediario titolare
Incaricati esterni: Software house Addetti pulizie Fornitore servizi di antifurto e videosorveglianza
Area parcellazione: Incaricati
Area contabilità e bilanci: Incaricati
Area pratiche e adempimenti amministrativi: Incaricati
Area dichiarazioni fiscali: Incaricati
Segreteria: Incaricat

Gli adempimenti privacy nell'attività dell'intermediario Entratel: gli incaricati

- La designazione degli incaricati per il trattamento dei dati e l'attribuzione dell'ambito di trattamento dati ad ognuno di essi consentito costituisce obbligo del titolare ai sensi dell'art. 30 del d. lgs. 196/2003, detto adempimento che deve risultare da documento scritto (art. 30, comma 2 d. lgs. 196/2003). L'atto di nomina dell'incaricato deve quindi essere esibito in sede di controllo. L'atto di nomina è valido se è data prova dell'avvenuta ricezione o presa visione (sufficiente anche l'esposizione dell'atto di nomina in una bacheca affissa all'interno dell'ufficio). E' consigliabile che l'atto di nomina, contenente le tipologie di dati trattati e le mansioni assegnate ai fini del trattamento dei dati, sia sottoscritto per presa visione dall'incaricato.
- La nomina degli incaricati ottempera alle previsioni dell'art. 11, comma 4 del D.M. 31/07/1998 e dell'art. 5 comma 4 del provvedimento 10/06/2009

Gli adempimenti privacy nell'attività dell'intermediario Entratel: il DPS

- I verificatori in sede di accesso chiedono se la struttura abilitata è in possesso del documento programmatico sulla sicurezza.
- La presenza del DPS aggiornato, almeno a data antecedente alla soppressione dell'obbligo di redazione consente ai verificatori di verificare anche l'organigramma Privacy, stante che nel documento devono essere indicati nel capitolo 2 il titolare, l'eventuale responsabile del trattamento, gli incaricati interni ed esterni.
- Le ispezioni effettuate dopo il 9 febbraio 2012 non inibiscono la possibilità di richiedere il DPS ove fosse stato redatto per gli anni precedenti.

Gli adempimenti privacy nell'attività dell'intermediario Entratel: il DPS

- Il DPS inoltre è strumento idoneo per identificare la valutazione dei rischi per la riservatezza dei dati trattati, nonché per valutare le misure minime di sicurezza adottate per prevenire i rischi.
- Il DPS consente anche di verificare l'inventario degli strumenti utilizzati per il trattamento.
  - I contenitori degli archivi cartacei
  - I contenitori degli archivi in formato elettronico (Server, personal computer, dispositivi elettronici di stampa, di memorizzazione)
  - Gli strumenti di disaster & recovery dei dati e la pianificazione delle attività volte a salvaguardare l'integrità dei dati trattati con strumenti elettronici
  - L'individuazione delle banche dati in cui sono raggruppati i dati trattati con strumenti elettronici e le policy di sicurezza per l'accesso alle stesse, al fine di valutarne la rispondenza all'incarico.
  - Le politiche di sensibilizzazione dei soggetti incaricati del trattamento con evidenza della pianificazione delle attività formative.

Le semplificazioni introdotte in materia di DPS

- Provvedimento Garante Privacy 27/11/2008 DPS semplificato
  - *Soggetti che possono avvalersi della semplificazione*
    Le modalità semplificate sono applicabili dai soggetti pubblici o privati che:
    a) utilizzano dati personali non sensibili o che trattano come unici dati sensibili riferiti ai propri dipendenti e collaboratori anche a progetto quelli costituiti dallo stato di salute o malattia senza indicazione della relativa diagnosi, ovvero dall'adesione a organizzazioni sindacali o a carattere sindacale;
    *b) trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese (*cfr. *art. 2083 cod. civ. e d.m. 18 aprile 2005, recante adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese, pubblicato nella Gazzetta Ufficiale 12 ottobre 2005, n. 238*).
- Esonero dall'obbligo di predisposizione del DPS con obbligo di dichiarazione sostitutiva sul rispetto delle misure minime di sicurezza (D.L. 70/2011).
  - Soggetti che possono avvalersi della semplificazione le imprese che trattano solo dati personali non sensibili e come unici dati sensibili quelli dei dipendenti , dei collaboratori anche se extracomunitari, e dei loro familiari (coniuge e parenti). In tale ipotesi, la tenuta del DPS è sostituita da un'autocertificazione resa ai sensi dell'art.47 del DPR 445/2000, circa il rispetto delle altre misure minime di sicurezza previste dal Disciplinare Tecnico allegato B al d. lgs. 196/2003.

Le semplificazioni introdotte in materia di DPS

- Con ‘art. 45 del d.lgs. n. 5 del 9/02/2012 la redazione e l’aggiornamento del DPS sono soppresse. Infatti la disposizione abroga:
  - L’art. 34, c. 1, lett. g del d.lgs. 196/2003, che prevedeva quale misura minima di sicurezza la tenuta di un aggiornato DPS
  - La regola n. 19 (paragrafi da 19.1 a 19.8) che stabilivano i presupposti , le modalità di redazione e i contenuti del DPS
  - La regola 26 del Disciplinare tecnico che imponeva al titolare del trattamento dati di riferire, nella relazione sulla gestione in merito all’avvenuto aggiornamento del DPS
  - L’art. 34, c.1-bis, del d.lgs. 196/2003, che disciplinava i casi per la sostituzione del DPS con l’autocertificazione resa dal titolare del trattamento.

Gli adempimenti privacy nell'attività dell'intermediario Entratel: la formazione degli incaricati.

- I soggetti incaricati del trattamento dati oltre a ricevere le indicazioni sull'ambito del trattamento, sulla metodologia di utilizzo degli strumenti elettronici per il trattamento dei dati, devono essere costantemente formati in merito alle responsabilità connesse alla condivisione o comunicazione dei dati trattati nello svolgimento delle proprie mansioni a persone non legittimate.
- La formazione inoltre deve consentire di acquisire e padroneggiare la conoscenza delle misure minime di sicurezza, connesse alla custodia delle credenziali per l'accesso ai sistemi informativi e alle banche dati, la conoscenza della policy della struttura connessa all'utilizzo degli strumenti elettronici e delle applicazioni software utilizzate.
- Le attività formative devono essere pianificate e devono essere attestate.

Le misure minime per il trattamento dei dati con strumenti elettronici.

- L'art. 11, comma 5 del D.M. 31/07/1998 impone agli organi di verifica di accertare le misure organizzative fisiche e logiche. Con riguardo al trattamento dei dati mediante strumenti elettronici le misure minime necessarie sono:
  - La gestione dell'autenticazione informatica nell'attività di accesso agli strumenti elettronici e alle banche dati e l'adozione di procedure di gestione delle credenziali di autenticazione (nome_utente e password).
  - L'utilizzo di un sistema di policy di autorizzazione informatica, che delinei la possibilità di accesso alle banche dati, in consultazione, inserimento, modifica e cancellazione dei dati.
  - L'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e agli addetti alla manutenzione degli strumenti elettronici, fornendo opportune e chiare istruzioni per l'effettiva protezione dei dati
  - La protezione dei sistemi informatici e dei dati con essi trattatati rispetto a trattamenti illeciti degli stessi, ad accessi non consentiti e all'inoculazione di programmi informatici dannosi.
  - Il costante aggiornamento degli strumenti elettronici, con particolare riguardo ai sistemi operativi e agli applicativi utilizzati per il trattamento dei dati, al fine di prevenirne la vulnerabilità e correggerne i difetti di programmazione, che possono provocare la perdita dei dati.
  - L'adozione di procedure per la custodia di copie di sicurezza, e la verifica dell'azione di ripristino dei dati salvati e dei sistemi informativi utilizzati per il trattamento dei dati, non trascurando le opportune istruzioni agli incaricati che sono preposti a questa importante funzione..
  - L'adozione di misure di protezione e ripristino specifiche per i dati sensibili e giudiziari, rispetto ad accessi abusivi e fornitura di istruzioni tecniche e organizzative per la custodia e l'uso di supporti rimovibili contenenti tali tipologie di dati.
  - La predisposizione di attestazioni adeguatamente sottoscritte di conformità da parte degli incaricati esterni, rispetto alla struttura del titolare, riguardanti il rispetto della privacy policy della struttura, nell'ambito dei loro interventi e/o trattamenti;
  - L'adozione di misure di sorveglianza e di controllo degli accessi finalizzate alla protezione e conservazione riservata dei dati trattati con strumenti diversi da quelli elettronici.

La policy privacy della postazione di lavoro

- Ogni postazione di lavoro deve essere impostata per consentire l'autenticazione dell'accesso ai dati e alle applicazioni. Gli incaricati devo dare prova di conoscere le regole per la conservazione e la modifica delle credenziali di accesso agli strumenti elettronici utilizzati per il trattamento.
- Le postazioni devono essere impostate per il blocco automatico dell'accesso in caso di periodo di inattività. Gli incaricati che utilizzano le postazioni informatiche in caso di abbandono della postazione devono conoscere le modalità per bloccarne l'accesso alle informazioni.
- L'incaricato deve dare prova di conoscere la policy della struttura con riguardo all'utilizzo della postazione di lavoro, l'utilizzo della posta elettronica per la comunicazione dei dati trattati, la non installazione di programmi in grado di consentire l'accesso non controllato ai dati.

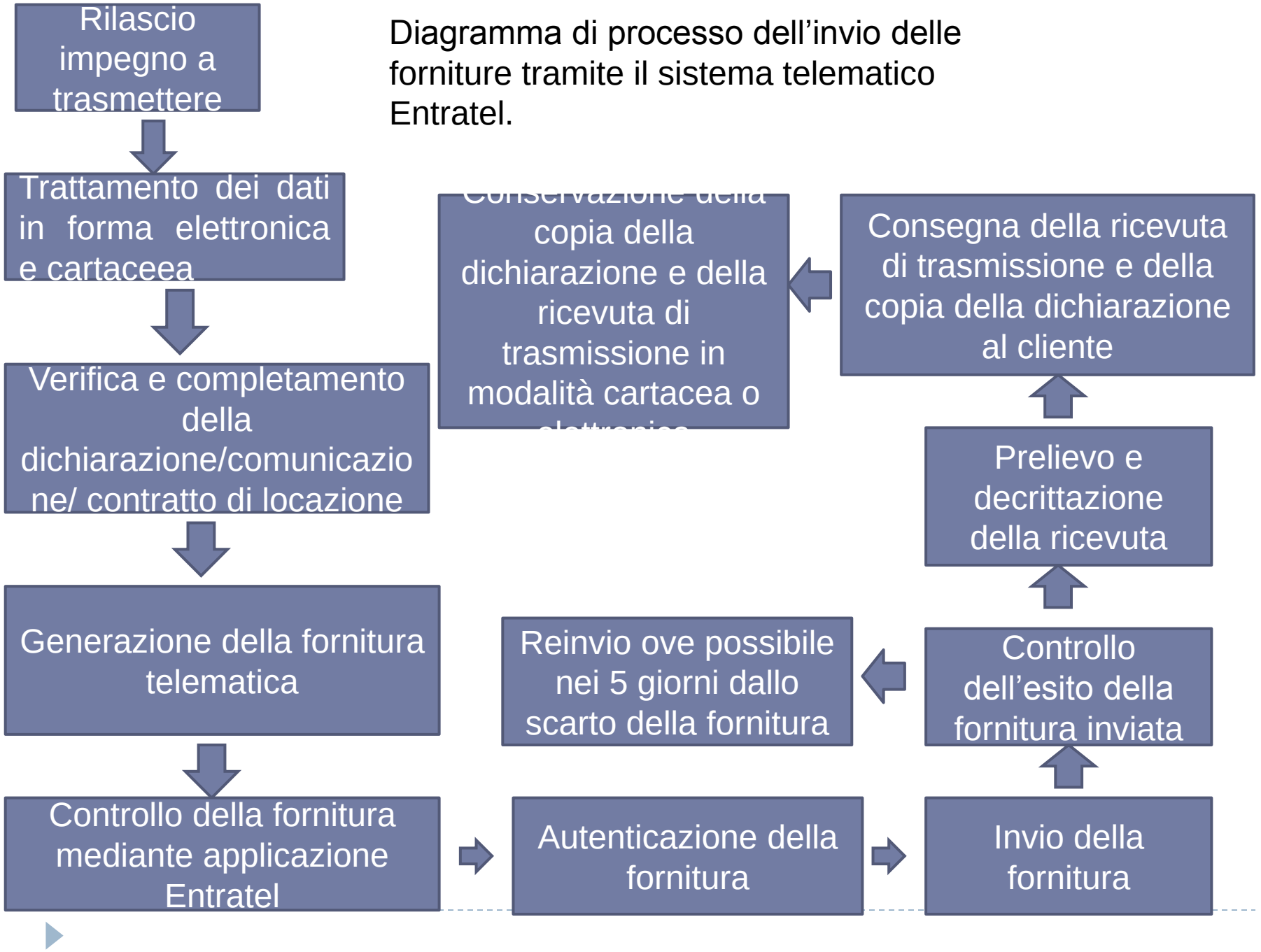
L’evidenza della strutturazione dei processi di utilizzo del Servizio Telematico Entratel

- Con riguardo all’utilizzo del sistema Telematico Entratel la struttura del titolare intermediario deve dare evidenza di essere uniformata al provvedimento del Garante della Privacy del 18/09/2008, che ha previsto l’attribuzione di credenziali personali ad ogni soggetto gestore e/o incaricato.
  - Pertanto ogni incaricato o gestore incaricato deve dare prova di conoscere le regole per la conservazione e l’utilizzo delle credenziali di autenticazione al servizio telematico Entratel.
  - Il gestore incaricato e/o l’incaricato deve dare prova di conoscere ed osservare le regole per la conservazione e l’utilizzo delle chiavi di autenticazione per crittografia delle forniture telematiche, nonché della busta contenente le chiavi per l’autenticazione iniziale e il pincode utile alla generazione delle chiavi di autenticazione delle forniture.

L’evidenza del processo di trattamento dei dati veicolati tramite il sistema telematico.

- In sede di verifica è bene esibire il documento interno illustrativo delle istruzioni interne per la gestione del procedimento di generazione delle forniture telematiche, del controllo della fornitura, dell’attività di autenticazione e invio delle forniture, nonché dell’attività di controllo della fase successiva all’invio della fornitura telematica, con riguardo al prelevamento e decrittazione delle ricevute di trasmissione delle dichiarazioni e delle comunicazione inviate tramite il sistema telematico Entratel. Per le strutture in cui l’attività non è curata direttamente dall’intermediario abilitato o dal gestore incaricato deve essere data prova della policy di autenticazione per l’accesso e la gestione degli archivi.
- Occorre dare prova della consegna dell’impegno alla trasmissione telematica delle dichiarazioni, delle comunicazioni e dei contratti di locazione.
- Occorre dare prova dell’attività di consegna della copia della dichiarazione sottoscritta e della ricevuta di trasmissione telematica.
- Occorre inoltre da prova della modalità di conservazione delle dichiarazioni, delle comunicazioni e dei contratti di locazione trasmessi, per quanto attiene la copia intermediario che costituisce l’originale del documento amministrativo per l’Agenzia delle Entrate.

Diagramma di processo dell'invio delle forniture tramite il sistema telematico Entratel.



La conservazione delle dichiarazioni trasmesse

- L'intermediario deve dare prova della conservazione della dichiarazione trasmessa e della ricevuta di trasmissione. La verifica deve fare emergere le politiche adottate per garantire l'accesso riservato e controllato all'archivio contenente la copia della dichiarazione e le scelte per la destinazione dell'8 e 5 per mille.
- La conservazione può essere effettuata anche mediante strumenti elettronici, con sottoscrizione digitale ed apposizione dell'evidenza informatica entro un anno dal termine per la trasmissione della dichiarazione.
- In caso di conservazione sostitutiva con strumenti elettronici della copia intermediario, occorre inviare l'impronta informatica della validazione temporale all'Agenzia delle Entrate.
- La documentazione dei documenti contenenti dati sensibili deve essere conservata in modo separato dalla restante documentazione archiviata nel fascicolo contenente la copia della dichiarazione dell'intermediario (sufficiente una busta chiusa acclusa al fascicolo).
- La documentazione trasmessa e la documentazione relativa alle procedure di controllo delle forniture deve essere conservata in spazi di cui deve essere data prova della protezione dall'accesso non autorizzato: locale o armadio protetto da chiusura con assegnazione della custodia delle chiavi.