Progetto GIT

La gestione associata dei tributi

Aspetti relativi alla privacy

COMUNE DI CREMA

Introduzione

Il presente documento si pone l'obiettivo di approfondire, in ottica privacy, i trattamenti di dati connessi alla gestione dei tributi quando tale funzione è svolta nella specifica forma organizzativa associata dell'Unione di comuni. Il documento si articola affiancando, ad una prima sezione teorica sui presupposti normativi e organizzativi funzionali allo sviluppo di un modello associato per la gestione dei tributi, una seconda sezione in cui si forniscono informazioni pratiche, procedure operative e schemi utili per gli adempimenti previsti dalle disposizioni normative.

La prima parte del documento è dedicata all'esame del quadro normativo generale, nel rispetto del quale vengono svolti i trattamenti di dati personali per le finalità di accertamento tributario e contributivo e di controllo qualitativo del dato catastale, e alla individuazione dei dati personali trattati e delle relative banche dati.

Vengono fissate alcune definizioni, contenute nel "Codice in materia dei dati personali" (di seguito Codice), utili per meglio comprendere i successivi contenuti del documento. Si esaminano i "Principi generali per il trattamento dei dati" e alcune "Regole ulteriori" che i soggetti pubblici, in qualità di "Titolari" del trattamento, devono rispettare per lo svolgimento delle proprie funzioni istituzionali adottando le misure di sicurezza previste dal Codice. Un focus specifico è dedicato alle operazioni di conservazione e comunicazione.

Si definisce il modello organizzativo che, attraverso la gestione associata di servizi, rappresenta una possibile risposta per fronteggiare le criticità tipicamente espresse dai piccoli comuni. La forma associativa considerata come riferimento per le riflessioni sull'applicazione della normativa sulla privacy è l'Unione di comuni.

Al fine di circoscrivere correttamente il modello di gestione associata dei tributi si ritiene necessario analizzare, anche alla luce delle finalità direttamente connesse alle specifiche

funzioni istituzionali (contrasto all'evasione fiscale, locale e erariale, cooperazione e interscambio di informazioni tra i diversi Servizi dell'Amministrazione comunale e cooperazione tra Amministrazioni Locali e Centrali) alcuni aspetti operativi connessi al trattamento dei dati, con particolare riguardo ai dati da inserire nella piattaforma informatica e alle procedure organizzativo–gestionali di alimentazione dei flussi. Alla luce di ciò sono individuati i principali dati personali oggetto di inserimento nel datawarehouse previsto dal Progetto Esecutivo GIT. I dati sono determinati con specifico riferimento a ciascuna tipologia di Segnalazione Particolare prevista all'interno di ogni ambito di intervento (ai sensi del punto 4 dell'art. 1 del Provvedimento del Direttore dell'Agenzia delle Entrate 3 dicembre 2007 "Ambiti di intervento e segnalazioni particolari").

Vengono illustrati alcuni importanti aggiornamenti che il modello di gestione dei tributi così definito, collocato all'interno di una Unione di Comuni, determina nell'impianto del sistema di gestione della privacy dei singoli comuni aderenti.

Il trattamento di dati personali, anche quando effettuato nell'ambito della gestione tributaria, comporta in capo al Titolare l'onere di ridurre al minimo 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. Il documento approfondisce le misure di sicurezza minime e idonee, distinguendole in relazione al soggetto che le deve adottare (Unione o singolo comune aderente).

Infine, si illustrano le fasi e gli strumenti (schemi-tipo) che caratterizzano il processo di adeguamento del "sistema Privacy" dell'Unione e dei singoli comuni aderenti, a seguito dell'attivazione del sistema di gestione tributaria in forma associata. L'obiettivo è quello di fornire un percorso utile per mettere in condizione l'Unione e i singoli comuni aderenti di tutelare gli interessi dei soggetti pubblici e privati che fanno affidamento sui trattamenti svolti dagli Enti, riducendo il rischio di eventi pregiudizievoli che possano danneggiare disponibilità, riservatezza e integrità del patrimonio di dati degli Enti.

Sommario

1

Dati, privacy e gestione associata

1.1 I presupposti normativi

Il decreto legge 31 maggio 2010 n. 78 convertito nella legge n. 122 del 30 luglio 2010 pone le premesse per il federalismo fiscale. Inoltre, individua le amministrazioni comunali quali soggetti fondamentali per il raggiungimento di obiettivi prioritari a livello nazionale. Esse possono svolgere attività di accertamento tributario e contributivo (art. 18) e di controllo qualitativo del dato catastale (art. 19). I Comuni possono individuare efficaci soluzioni organizzative e istituzionali con l'adozione di una serie di procedure di accertamento tributario e di controllo del dato catastale e della sua correlazione con l'anagrafe estesa dei cittadini e delle imprese.

Inoltre, la norma citata impone ai Comuni con popolazione inferiore a 5000 abitanti di gestire in forma associata i servizi relativi ad alcune funzioni definite fondamentali. Il modello associativo con un forte comune capofila rappresenta un contributo rilevante per orientarsi verso un più solido e stabile accrescimento della qualità ed equità nell'esercizio delle funzioni catastali e della fiscalità locale. Le esperienze di tipo associativo già realizzate testimoniano la necessità di una forte e coordinata azione di sponsorship per supportare il passag-

gio da una fase di generico interesse a una di concreta attivazione di processi di cambiamento istituzionale e organizzativo.

Al fine di dare concreta attuazione a tali funzioni, il Comune sviluppa un modello che prevede il coinvolgimento dei seguenti Servizi/Settori (che possono variare in considerazione delle singole specifiche strutture organizzative adottate):

- Territorio, e Sportello Unico per l'edilizia
- Sistemi Informativi
- Tributi
- Anagrafe
- Commercio
- Polizia Localex

1.2 Le banche dati

Conseguentemente, le banche dati interne utilizzabili per le attività di accertamento, classificate per tematica, possono essere le seguenti:

- Anagrafe
- Edilizia
- Tributi
- Polizia Locale
- Urbanistica

- Licenze Commercio

Le banche dati esterne, classificate per ambito, sono le seguenti:

- Camera di Commercio: riguarda i dati relativi alle imprese sul territorio comunale
- Agenzia del Territorio (Catasto – DOCFA): riguarda dati catastali connessi a dati personali
- Agenzia delle Entrate: (SIATEL – Successioni – Locazioni – Redditi) per quanto riguarda i dati di reddito collegati anche ad informazioni catastali

1.3 I dati trattati

I dati da trattare per le funzioni previste devono essere selezionati facendo riferimento a ciascuna tipologia di Segnalazione Particolare prevista all'interno di ogni ambito di intervento (ai sensi del punto 4 dell'art. 1 del Provvedimento del Direttore dell'Agenzia delle Entrate 3 dicembre 2007 "Ambiti di intervento e segnalazioni particolari"):

A) Commercio e Professioni:

1. Svolgimento attività senza Partita IVA
2. Svolgimento attività diversa da quella rilevata
3. Affissione pubblicitaria abusiva
4. Affissione pubblicitaria non abusiva
5. Ente non commerciale con attività lucrativa "prevalente"

B) Urbanistica e Territorio:

1. Opere di lottizzazione in funzione strumentale alla cessione di terreni
2. Cessione di fabbricato grezzo in luogo cessione del relativo terreno edificabile
3. Professionista o imprenditore che ha partecipato ad operazioni di abusivismo edilizio

C) Proprietà edilizie e Patrimonio immobiliare:

1. Proprietà o diritto reale non indicati in dichiarazione
2. Proprietà o diritto reale in assenza di contratti registrati
3. Accertamento per omessa dichiarazione ICI
4. Accertamento per omessa dichiarazione TARSU/TIA
5. Revisione di rendita catastale ex art. 1, comma 336 Legge 311/2004

D) Residenze fittizie all'estero:

1. Esito negativo del Procedimento di conferma espatrio
2. Domicilio ex art. 43, commi 1 e 2 C.C.(e vigilanza nel triennio ex art.83, comma 16 D.L. 112/2008)

E) Disponibilità di beni indicativi di capacità contributiva:

1. Abitazioni principali e secondarie
2. Soggetti residenti in zone di pregio della città
3. Spese per ristrutturazioni immobiliari
4. Collaboratori familiari a tempo pieno e conviventi
5. Possesso beni di lusso non inerenti reddito impresa

2

Il trattamento dei dati

2.1 Definizioni

Si considerano alcune definizioni contenute nell'art. 4 del D. Lgs. 30 giugno 2003 n. 196 "Codice in materia dei dati personali" (di seguito Codice) e riportate di seguito, utili per meglio comprendere i successivi contenuti del documento.

Trattamento: qualunque operazione o complesso di operazioni, effettuati 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, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

Dato personale: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato;

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;

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Titolare: 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: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Incaricato: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile;

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

Comunicazione: trattamento che consiste nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

Banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

Comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

Reti di comunicazione elettronica: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

Misure minime di sicurezza: 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 del Codice;

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

Profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

2.2 Regole per il trattamento dei dati

In termini generali, i soggetti pubblici (cd. "Titolari del trattamento") che trattano dati personali per lo svolgimento delle proprie funzioni istituzionali non devono richiedere il consenso dell'interessato. Tuttavia ciò non attribuisce, ai soggetti pubblici che trattano dati personali per lo svolgimento delle proprie funzioni istituzionali, alcun margine di discrezionalità nei trattamenti effettuati. I soggetti pubblici devono rispettare i "Principi generali per il trattamento dei dati" e alcune "Regole ulteriori per i soggetti pubblici" adottando le misure di sicurezza previste.

2.3 Le finalità istituzionali

Ai sensi del D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" (di seguito "Codice"), il primo requisito che occorre verificare riguarda la riconducibilità alle finalità istituzionali dell'ente locale di quelle attività svolte dagli Uffici comunali per il conseguimento delle finalità di partecipazione del Comune al contrasto all'evasione fiscale ed

all'accertamento dei Tributi erariali che implicano il trattamento di dati personali ed identificativi.

Le attività svolte dagli Uffici comunali per il conseguimento delle finalità di partecipazione del Comune al contrasto all'evasione fiscale ed all'accertamento dei Tributi erariali implicano il trattamento di dati personali ed identificativi. Ai sensi del D.lgs n. 196/2003 "Codice in materia di protezione dei dati personali" (d'ora in poi Codice), la fonte normativa primaria che attribuisce al Comune tali competenze e ne legittima l'esercizio delle funzioni è rinvenibile nell'art. 1 del D.L. 30 settembre 2005, n. 203 (Convertito dalla legge n. 248/2005) così come da ultimo modificato dall'art. 18, comma 5 del D.L. 31 maggio 2010 n. 78 (Convertito con Legge 30 luglio 2010 n. 122). Fonti secondarie ed attuative del citato articolo sono i Provvedimenti del Direttore dell'Agenzia delle Entrate del 3 dicembre 2007 e N. 2008/175466 del 26 novembre, Decreto Direttore Agenzia del Territorio 13/11/2007 e Provvedimento Agenzia del Territorio del 16/6/2008.

In seguito per dare attuazione concreta a tali normative l'Agenzia delle Entrate (Direzione Regionale Lombardia) ha stipulato con l'ANCI in data 27 novembre 2008 una convenzione finalizzata a favorire la collaborazione tra Agenzia e Comuni ed in seguito una convenzione specifica con il Comune di Crema approvata dalla Giunta Comunale in data 22 novembre 2010 con delibera 2010/434. L'oggetto di tale convenzione consiste nella definizione di un programma locale di recupero dell'evasione dei tributi statali in stretta collaborazione con gli uffici dell'Agenzia delle Entrate competenti per l'attività di accertamento ed ove richiesto con la Direzione Regionale della Lombardia e delle modalità concordate di reciproco intervento.

2.4 Principi generali

In base ai "Principi generali", posto che i dati devono essere trattati in modo lecito e secondo correttezza, gli scopi per cui i dati sono raccolti e registrati devono essere determinati,

espliciti e legittimi. L'utilizzo dei dati in altre operazioni è consentito solo se tali operazioni sono compatibili con gli scopi di raccolta e registrazione. I dati trattati devono essere esatti (e, se necessario, aggiornati), ma devono anche essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e trattati. Infine, i dati trattati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2.5 Regole ulteriori

Il trattamento, da parte degli Uffici comunali, di dati diversi da quelli sensibili e giudiziari è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

Il trattamento, da parte degli Uffici comunali, di dati sensibili o giudiziari è consentito solo se autorizzato da espressa disposizione di legge nella quale siano specificati:

- i tipi di dati che possono essere trattati
- i tipi di operazioni eseguibili
- le finalità di rilevante interesse pubblico perseguite.

Nei casi in cui una disposizione di legge specifichi la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili o giudiziari e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g) del Codice (anche su schemi tipo).

Nell'ambito delle attività sottese al progetto GIT i dati identificativi oggetto di trattamento sono sostanzialmente: dati anagrafici, codice fiscale e partita IVA.

2.6 Misure di sicurezza: protezione dati

Il Codice fornisce maggiori garanzie nel trattamento dei dati personali senza per questo compromettere la trasparenza e la semplificazione dell'azione amministrativa.

Le disposizioni contenute nel Codice impongono l'assolvimento di una serie di adempimenti sia formali che sostanziali, tra cui gli obblighi che attengono alla sicurezza. Per quanto attiene agli obblighi generali di sicurezza il Codice – art. 31 – stabilisce che i dati personali devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, attraverso l'adozione di idonee e preventive misure di sicurezza atte a ridurre al minimo i rischi di:

- distruzione o perdita anche accidentale dei dati
- di accesso non autorizzato
- trattamento non consentito
- trattamento non conforme alle finalità della raccolta

Per quanto riguarda gli obblighi "specifici" di sicurezza il Codice presenta un elenco di misure tecnologiche, organizzative e procedurali (artt. da 33 a 36 e Allegato B – Disciplinare tecnico in materia di misure minime di sicurezza) al fine di assicurare il livello minimo di protezione dei dati.

2.7 Le misure minime

Le misure minime riguardano sia trattamenti svolti con strumenti elettronici che senza strumenti elettronici.

Per i **trattamenti svolti con strumenti elettronici** l'art. 34 del Codice prevede:

a. l'autenticazione informatica;

b. l'adozione di procedure di gestione delle credenziali di autenticazione;

c. l'utilizzazione di un sistema di autorizzazione;

d. l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e. la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f. l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g. la tenuta di un aggiornato documento programmatico sulla sicurezza;

h. l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Rispetto ai **trattamenti effettuati senza l'ausilio di strumenti elettronici** l'art. 35 contempla:

a. l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b. la previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c. la previsione di procedure per la conservazione di atti contenenti dati sensibili o giudiziari in archivi ad accesso selezionato e la disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Tutte le misure descritte devono essere implementate seguendo le modalità contenute nel citato "Disciplinare tecnico in materia di misure minime di sicurezza", al fine di soddisfare gli obiettivi "legali" di sicurezza, riconducibili nell'ambito dei sistemi informativi:

- all'integrità intesa come salvaguardia dell'accuratezza, completezza dei dati
- alla riservatezza nel senso che occorre garantire la protezione dei dati da accessi non autorizzati
- alla disponibilità quale garanzia della possibilità di utilizzare le informazioni quando richiesto dagli utenti/operatori

2.8 Conservazione

I dati che consentano l'identificazione dell'interessato, devono essere conservati nella forma e per un periodo di tempo strettamente necessari agli scopi per i quali essi sono stati raccolti e trattati.

2.9 Comunicazione

Nell'ambito delle attività di accertamento fiscale, tributario e di altra natura si prevede lo scambio di dati, diversi da quelli sensibili e giudiziari, da e verso enti esterni all'amministrazione. Tale operazione si configura, secondo il Codice, come "comunicazione"

ed è ammessa solo se prevista da una norma di legge o di regolamento. Sotto tale profilo risultano di particolare rilievo i trattamenti connessi alla trasmissione dei dati tra Comune e Agenzia delle Entrate oppure tra Comune e Agenzia del Territorio.

Sempre nell'ambito delle attività di accertamento fiscale, tributario e di altra natura lo scambio di dati, diversi da quelli sensibili e giudiziari, tra Servizi/Strutture che sono individuati quali Incaricati al trattamento dal medesimo Titolare non configura alcuna "comunicazione". In tali casi si applicano i "Principi generali per il trattamento dei dati" e le "Regole ulteriori per i soggetti pubblici" precedentemente illustrate, nel rispetto delle misure di sicurezza.

3

L’unione di comuni e la gestione associata dei tributi

L’esistenza di una forte quantità di piccoli comuni è uno dei tratti caratterizzanti la pubblica amministrazione lombarda e, in generale, italiana.

Le minori dimensioni delle amministrazioni locali attenuano, ma non eliminano l’intrinseca complessità del governo e gestione della fiscalità locale.

La natura dei problemi da affrontare sono, infatti, paragonabili a quelli rinvenibili in amministrazioni

comunali di più ampie dimensioni:

- attuazione del federalismo municipale, come condizione per disporre di adeguate risorse, in una situazione di sostanziale riduzione dei trasferimenti;
- necessità di rispondere alle sollecitazioni delle comunità locali che hanno richiesto progressi della qualità nei rapporti con i contribuenti, economicità dell’azione pubblica e raggiungimento di elevati livelli di equità fiscale in tempi particolarmente accelerati;
- sviluppo dell'integrazione con le attività svolte da altri soggetti pubblici impegnati nell’adeguare complessivamente il sistema fiscale. Le amministrazioni

comunali rappresentano, in applicazione del principio di sussidiarietà, un nodo strategico della rete di istituzioni pubbliche e private. In particolare assume una rilevanza significativa la collaborazione con l'Agenzia delle entrate in tema di fornitura didati utili all'accertamento della posizione contributiva delle persone.

- I piccoli comuni sono esposti più di altri alla complessità generata da tali sfide a causa della difficoltà di agire su fattori quali l'organizzazione, il personale, le tecnologie per garantire:
- la possibilità di governare l'innovazione gestionale in tema di federalismo municipale e di sviluppo delle banchedati informative che rappresentano la condizione imprescindibile di ogni percorso di cambiamento con modalità, per larga parte,indipendenti dalle specificità delle normative vigenti;
- l'efficace ed efficiente svolgimento dei processi di accertamento, liquidazione e riscossione secondo le leggi in vigore, che implicano la presenza di capacità d'investimento e di competenze amministrative, organizzative e di sviluppo dei sistemi informativi, di natura gestionale e operativa, difficilmente reperibili nei comuni di minori dimensioni;
- una più adeguata forza contrattuale nel negoziare con soggetti terzi, quali fornitori e altre amministrazioni, condizioni di collaborazione vantaggiosa.

La gestione associata di servizi rappresenta una possibile risposta per fronteggiare le criticità tipicamente espresse dai piccoli comuni.

3.1 Un nuovo interesse per le gestioni associate

Le gestioni associate, in questo periodo, sono oggetto, da parte di amministratori comunali e responsabili della gestione, di un rinnovato interesse.

In primo luogo, nell'ambito delle amministrazioni comunali di piccola dimensione, si è giunti, rispetto anche a un recente passato, a un'attenta considerazione delle gestioni associate

volontarie quale risposta possibile a situazioni critiche connesse alla difficoltà di sostenere economicamente un'equilibrata declinazione dei principi di sussidiarietà e di adeguatezza. La collaborazione intercomunale viene certamente considerata come un'opportunità che può assumere un ruolo di vitale importanza per garantire il mantenimento e la rimodulazione dei servizi erogati a livello locale e legittimare la rappresentanza politica, ma anche fonte di problematicità e costi, soprattutto necessari per l'avvio del cambiamento.

In secondo luogo, le modificazioni normative che introducono, per i piccoli comuni, il concetto di obbligatorietà delle gestioni associate per tutte le funzioni o per quelle fondamentali inducono la necessità di garantire una risposta istituzionale nel breve/medio periodo. Dopo anni di sostanziale inerzia e disorganicità nella definizione di normative nazionali e regionali, la nuova disciplinarelativa alle gestioni associate (DL 78/2010 e al DL 138/2011) il suo tratto distintivo, ha determinato una necessaria attenzione all'applicazione di norme che sono vissute con atteggiamenti ambivalenti e contraddittori anche nell'ambito della medesima situazione. Ne ricordiamo alcuni:

- un obbligo da ottemperare con limitati ripensamenti delle consuete modalità d'intervento sull'organizzazione e sui sistemi di gestione, in modo anche da ridurre i rischi di esposizione a conseguenze negative in seguito ad azioni da parte degli organismi di controllo;
- un'occasione che consente di attuare reali disegni di cambiamento altrimenti problematici nei contesti locali dove le fonti d'influenza sulle decisioni sono significativamente distribuite;
- un evento verso il quale attuare azioni di forte protesta, fino ad arrivare a forme di disobbedienza manifesta.

L'impatto della normativa ha innescato anche nelle amministrazioni regionali un'attenzione particolare al tema delle gestioni associate per quanto riguarda la necessità di:

- accompagnare e incentivare efficacemente lo sviluppo della collaborazione nelle amministrazioni locali;

- intervenire sulla legislazione regionale per configurare un coerente sistema normativo sulle gestioni associate coerente con le prerogative della legislazione nazionale e attento alle specificità locali.

3.2 La gestione associata e la fiscalità locale

Le gestioni associate relative alla fiscalità comunale riguardano, in primo luogo, i servizi rivolti alla comunità locale:

- servizi tributari: ICI, TARSU, tributi minori;
- servizi di riscossione delle tariffe;
- servizi catastali.

In secondo luogo, sono associabili i servizi offerti ad altre istituzioni, come ad esempio all'Agenzia delle Entrate. Rientrano in questa tipologia di azione l'invio delle segnalazioni qualificate e lo scambio di accertamenti sintetici tra Agenzia e comuni.

In terzo luogo, sono da considerare come parte integrante di un disegno di collaborazione efficace i servizi di gestione delle risorse informative, economico finanziarie e di personale che rappresentano le condizioni operative per erogare le prime due tipologie di servizi.

3.3 Le Unioni di comuni come forma di gestione associata

Nel presente documento la forma associativa che sarà considerata come riferimento per le riflessioni sull'applicazione della normativa sulla privacy è l'Unione di comuni.

L’Unione di comuni rappresenta, nell’ambito dei principi generali di regolazione della cooperazione interistituzionaleinseriti nel Testo unico sull’ordinamento delle autonomie locali, una possibile risposta per fronteggiare alcune delle criticità tipicamente espresse dai piccoli comuni. Il Testo unico presenta nell’articolo 32 le specifiche norme relative alle Unioni di comuni.

Articolo 32 Testo unico Enti locali

Unioni di comuni

1. Le unioni di comuni sono enti locali costituiti da due o più comuni di norma contermini, allo scopo di esercitare congiuntamente una pluralità di funzioni di loro competenza.

2. L'atto costitutivo e lo statuto dell'unione sono approvati dai consigli dei comuni partecipanti con le procedure e la maggioranza richieste per le modifiche statutarie. Lo statuto individua gli organi dell'unione e le modalità per la loro costituzione e individua altresì le funzioni svolte dall'unione e le corrispondenti risorse.

3. Lo statuto deve comunque prevedere il presidente dell'unione scelto tra i sindaci dei comuni interessati e deve prevedere che altri organi siano formati da componenti delle giunte e dei consigli dei comuni associati, garantendo la rappresentanza delle minoranze.

4. L'unione ha potestà regolamentare per la disciplina della propria organizzazione, per lo svolgimento delle funzioni ad essa affidate e per i rapporti anche finanziari con i comuni.

5. Alle unioni di comuni si applicano, in quanto compatibili, i princìpi previsti per l'ordinamento dei comuni. Si applicano, in particolare, le norme in materia di composizione degli organi dei comuni; il numero dei componenti degli organi non può comunque eccedere i limiti previsti per i comuni di dimensioni pari alla popolazione complessiva dell'ente. Alle unioni competono gli introiti derivanti dalle tasse, dalle tariffe e dai contributi sui servizi ad esse affidati.

L'Unione di comuni si propone come un dispositivo istituzionale stabile sul lungo periodo che regola l'integrazione:

- delle forme di rappresentanza politica dei comuni aderenti;

- dell'offerta di servizi a una comunità locale;
- delle iniziative di animazione e promozione economica, sociale e ambientale in ambito locale e delle espressioni delle culture delle popolazioni coinvolte.

L'Unione di comuni può essere costruita solo attraverso un percorso nel quale si confrontano più coalizioni di interessi a partire dall'innesco del percorso determinato da un gruppo locale di agenti del cambiamento.

In linea generale, se le Unioni sono equiparate ad altri enti locali tradizionalmente consolidati, a loro si applicano tutte le disposizioni concernenti tali enti locali, senza bisogno d'ulteriori precisazioni e senza l'emanazione di specifiche norme di rinvio, così come recita l'art. 32, comma 5 del Testo Unico.

Per quanto riguarda la potestà statutaria e regolamentare, all'Unione è attribuita soltanto la potestà regolamentare relativa alla disciplina della propria organizzazione, per lo svolgimento delle funzioni ad essa affidate, e dei rapporti con le amministrazioni comunali che la costituiscono.

Lo schema di atto costitutivo e lo statuto dell'Unione sono approvati dai consigli dei comuni coinvolti partecipanti e con la maggioranza richiesta per le modifiche statutarie (Testo Unico art. 32, comma 2).

L'Unione è, dunque, un ente derivato nel quale le norme statutarie sono suscettibili di procurare gli effetti desiderati solo se ricevono l'adesione da parte di tutte le amministrazioni comunali che in quell'Unione si riconoscono.

Allo statuto è affidato il compito di definire l'assetto degli organi politici e le modalità della loro costituzione ed elezione. Nello statuto debbono essere specificate le funzioni da gestire in forma associata e disciplinate le modalità di acquisizione e utilizzo delle risorse finanziarie umane e strumentali.

4

Il trattamento dei dati per la gestione tributaria nel modello associato

Al fine di definire correttamente il modello di gestione associata dei tributi si è ritenuto necessario analizzare, anche alla luce delle finalità direttamente connesse alle specifiche funzioni istituzionali (contrasto all'evasione fiscale, locale e erariale, cooperazione e interscambio di informazioni tra i diversi Servizi dell'Amministrazione comunale e cooperazione tra Amministrazioni Locali e Centrali) alcuni aspetti operativi connessi al trattamento dei dati, con particolare riguardo ai dati da inserire nella piattaforma informatica e alle procedure organizzativo–gestionali di alimentazione dei flussi.

Nell'ambito delle attività di gestione dei tributi sono esclusi i trattamenti di dati sensibili e/o giudiziari. I dati oggetto di trattamento sono sostanzialmente: i dati anagrafici, codice fiscale e partita IVA. In proposito il Garante privacy ha formulato il parere 25 luglio 2007 "Modalità di partecipazione dei Comuni all'accertamento fiscale", con cui prevede la trasmissione dai Comuni all'agenzia delle entrate dei dati appena elencati. Per quanto riguarda le materie di accertamento connesse all'Agenzia del territorio, il Garante con il citato parere del 25 luglio 2007 rimandava ad un successivo provvedimento dell'Agenzia del territorio la

definizione delle modalità per la fruizione dei dati necessari. Sul punto, non si rilevano successivi provvedimenti da parte dell'Agenzia del Territorio né tanto meno da parte del Garante. Tuttavia, considerato che la tematica si inquadra nell'ambito del più generale tema degli accertamenti, i trattamenti si possono ritenere legittimi nei limiti dei principi di necessità, proporzionalità, pertinenza e non eccedenza sanciti dal Codice privacy.

4.1 Banche dati interessate

Le banche dati interne utilizzate per le attività di accertamento, raggruppate per tematica, sono le seguenti:

Anagrafe: per il popolamento iniziale del datawarehouse le informazioni anagrafiche (generalità e vicende anagrafiche) saranno comunicate dal Servizio Anagrafe al Responsabile del Progetto, secondo le regole e i limiti in materia anagrafica (poiché non costituisce duplicazione di database anagrafico, e non consente l'accesso diretto alla banca dati dell'anagrafe), al fine di consentire i processi di bonifica massiva in corso presso il Servizio Tributi quale attività propedeutica alle successive attività di partecipazione del comune aderente al contrasto all'evasione fiscale ed all'accertamento dei tributi. La comunicazione dei dati dovrà avvenire in modo sicuro, in modalità elettronica, nel rispetto delle misure di sicurezza. Periodicamente, al fine di garantire la qualità e l'aggiornamento dei dati e come già previsto dalla normativa vigente, i dati relativi alle variazioni anagrafiche saranno comunicate dal Servizio Anagrafe al Responsabile del Progetto secondo le regole e i limiti in materia anagrafica in modo sicuro, in modalità elettronica, nel rispetto delle misure di sicurezza.

Edilizia privata: per il popolamento iniziale del datawarehouse, al fine di consentire i processi di bonifica massiva in corso presso il Servizio Tributi quale attività propedeutica alle successive attività di partecipazione del comune aderente al contrasto all'evasione fiscale ed all'accertamento dei tributi, e successivamente al fine di garantire la qualità e

l'aggiornamento dei dati, le informazioni necessarie vengono raccolte dal Servizio competente che trasferirà i dati al datawarehouse mediante il Responsabile del Progetto in formato elettronico, nel rispetto delle misure di sicurezza.

Tributi: per il popolamento iniziale del datawarehouse, al fine di consentire i processi di bonifica massiva in corso presso il Servizio Tributi quale attività propedeutica alle successive attività di partecipazione del comune aderente al contrasto all'evasione fiscale ed all'accertamento dei tributi, e successivamente al fine di garantire la qualità e l'aggiornamento dei dati, i dati necessari relativi ad ICI, TARSU, COSAP saranno forniti dal Servizio competente al Responsabile del Progetto. La consegna dei dati dovrà avvenire in formato elettronico, nel rispetto delle misure di sicurezza..

Polizia Locale: per il popolamento iniziale del datawarehouse, al fine di consentire i processi di bonifica massiva in corso presso il Servizio Tributi quale attività propedeutica alle successive attività di partecipazione del comune aderente al contrasto all'evasione fiscale ed all'accertamento dei tributi, e successivamente al fine di garantire la qualità e l'aggiornamento dei dati, i dati necessari relativi ad accertamenti di abusivismo ed altre violazioni, dovranno essere trasmessi dal Servizio competente al Responsabile del Progetto in formato elettronico, nel rispetto delle misure di sicurezza.

Pianificazione territoriale e ambientale: per il popolamento iniziale del datawarehouse, al fine di consentire i processi di bonifica massiva in corso presso il Servizio Tributi quale attività propedeutica alle successive attività di partecipazione del comune aderente al contrasto all'evasione fiscale ed all'accertamento dei tributi, e successivamente al fine di garantire la qualità e l'aggiornamento dei dati, le informazioni relative prevalentemente al piano regolatore generale e alle eventuali varianti, che fanno riferimento a dati personali compatibili con la finalità perseguita, potranno essere trasferite dal Servizio competente al Responsabile del Progetto in formato elettronico, nel rispetto delle misure di sicurezza.

Licenze Commercio: per il popolamento iniziale del datawarehouse, al fine di consentire i processi di bonifica massiva in corso presso il Servizio Tributi quale attività propedeutica alle successive attività di partecipazione del comune aderente al contrasto all'evasione fiscale ed all'accertamento dei tributi, e successivamente al fine di garantire la qualità e

l'aggiornamento dei dati, il Servizio competente invierà i dati al Responsabile del Progetto in formato elettronico, nel rispetto delle misure di sicurezza.

4.2 I dati trattati

Di seguito si elencano i principali dati personali ed identificativi oggetto di inserimento nel datawarehouse previsto dal Progetto Esecutivo GIT. I dati sono elencati con specifico riferimento a ciascuna **tipologia di Segnalazione Particolare** prevista all'interno di ogni ambito di intervento (ai sensi del punto 4 dell'art. 1 del Provvedimento del Direttore dell'Agenzia delle Entrate 3 dicembre 2007 "Ambiti di intervento e segnalazioni particolari").

A) COMMERCIO E PROFESSIONI:

1. Svolgimento attività senza Partita IVA: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico e, per gli immobili a qualsiasi titolo detenuti per lo svolgimento delle attività professionali e/o commerciali, Foglio e Mappale;
2. Svolgimento attività diversa da quella rilevata: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico e, per gli immobili a qualsiasi titolo detenuti per lo svolgimento delle attività professionali e/o commerciali, Foglio e Mappale;
3. Affissione pubblicitaria abusiva: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico;
4. Affissione pubblicitaria non abusiva: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico;
5. Ente non commerciale con attività lucrativa "prevalente": Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico e, per gli immobili a qualsiasi titolo detenuti per lo svolgimento delle attività istituzionali lucrative, Foglio e Mappale, subalterno e particella.

B) URBANISTICA E TERRITORIO:

1. Opere di lottizzazione in funzione strumentale alla cessione di terreni: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e particella;

2. Cessione di fabbricato grezzo in luogo cessione del relativo terreno edificabile: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico , Foglio, Mappale, subalterno e particella;

3. Professionista o imprenditore che ha partecipato ad operazioni di abusivismo edilizio: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e particella;

C) PROPRIETÀ EDILIZIE E PATRIMONIO IMMOBILIARE:

1. Proprietà o diritto reale non indicati in dichiarazione: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e Particella;

2. Proprietà o diritto reale in assenza di contratti registrati: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e Particella;

3. Accertamento per omessa dichiarazione ICI: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e Particella;

4. Accertamento per omessa dichiarazione TARSU/TIA: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e Particella;

5. Revisione di rendita catastale ex art. 1, comma 336 Legge 311/2004: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e Particella;

D) RESIDENZE FITTIZIE ALL'ESTERO:

1. Esito negativo del Procedimento di conferma espatrio: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico;

2. Domicilio ex art. 43, commi 1 e 2 C.C.(e vigilanza nel triennio ex art.83, comma 16 D.L. 112/2008): Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio;

E) DISPONIBILITÀ DI BENI INDICATIVI DI CAPACITÀ CONTRIBUTIVA:

1. Abitazioni principali e secondarie: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e Particella;

2. Soggetti residenti in zone di pregio della città: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e Particella;

3. Spese per ristrutturazioni immobiliari: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico, Foglio, Mappale, subalterno e Particella;

4. Collaboratori familiari a tempo pieno e conviventi: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico e, per gli immobili a qualsiasi titolo detenuti, Foglio e Mappale;

5. Possesso beni di lusso non inerenti reddito impresa: Nome, Cognome, Codice Fiscale, Partita IVA, Via e n. civico e, per gli immobili a qualsiasi titolo detenuti, Foglio e Mappale.

5

Il sistema di gestione della privacy nell'unione di comuni

Il modello di gestione dei tributi definito nei paragrafi precedenti, che si colloca all'interno di una Unione di Comuni, determina alcuni importanti aggiornamenti nell'impianto del sistema di gestione della privacy dei singoli comuni aderenti e pone alcuni specifici obblighi in capo all'Unione. Il primo aspetto da rilevare consiste nel trasferimento della titolarità del trattamento dei dati per le finalità di gestione tributaria dal singolo comune aderente all'Unione. Pertanto le decisioni (e le conseguenti responsabilità) in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza, competono all'Unione.

Da ciò discende che spetta all'Unione l'eventuale designazione del Responsabile del trattamento dei dati per le finalità di gestione tributaria, individuandolo tra quei soggetti che per esperienza, capacità ed affidabilità forniscano garanzia di rispetto delle disposizioni vigenti in materia di trattamento dei dati, compreso il profilo relativo alla sicurezza. A tal fine, nulla esclude che il Responsabile del trattamento dei dati per le finalità di gestione tributaria coincida con il Responsabile dell'Ufficio. Il Titolare individua analiticamente i compiti affidati al Responsabile, specificandoli per iscritto e vigila, anche tramite verifiche periodiche, sulla osservanza delle disposizioni normative e delle istruzioni.

Analogamente il Titolare (o il Responsabile eventualmente designato) individua gli Incaricati, ovvero i soggetti autorizzati a compiere, sotto la diretta autorità del Titolare o dell'eventuale Responsabile e attenendosi alle istruzioni impartite, operazioni di trattamento per le finalità di gestione tributaria. Il Titolare (o il Responsabile) individua gli Incaricati tra i dipendenti che compongono la propria dotazione organica, ma anche tra i soggetti eventualmente assegnati all'Unione (in distacco e/o comando) dai comuni aderenti. I singoli comuni aderenti che trasferiscano all'Unione la funzione tributaria o che assegnino all'Unione (in distacco e/o comando) proprio personale provvedono ad aggiornare l'ambito del trattamento consentito ai singoli Incaricati, in occasione della verifica periodica (almeno una volta l'anno.

In coerenza con questi cambiamenti nella configurazione del "sistema Privacy", il singolo comune aderente e l'Unione aggiornano il contenuto dell'Informativa che deve essere fornita all'interessato per renderlo edotto di:

a. le finalità e le modalità del trattamento cui sono destinati i dati;
b. la natura obbligatoria o facoltativa del conferimento dei dati;
c. le conseguenze di un eventuale rifiuto di rispondere;
d. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e. i diritti di cui all'articolo 7 del Codice Privacy;
f. gli estremi identificativi del Titolare e, se designati, del Responsabile. Quando il titolare abbia designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7 del Codice Privacy, è indicato tale responsabile.

Le operazioni di trattamento per le finalità di gestione tributaria e il modello organizzativo associato nel quale si sviluppano implicano l'utilizzo massivo di dati, rendendo critiche atti-

vità tecniche “ordinarie” quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware/software. Tali attività, che costituiscono comunque trattamento di dati personali, possono comportare l’accesso diretto (anche fortuito) a intere banche-dati rendendo particolarmente qualificato il rischio di reati quali l’accesso abusivo al sistema informatico o telematico (art. 615 ter codice penale), di frode informatica (art. 640 ter), di danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinques).

Queste considerazioni richiamano l’attenzione sull’opportunità, da parte dell’Unione, di adottare idonee misure volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, specialmente se riconducibili all’abuso della qualità di amministratore di sistema o di funzioni tecniche ad esso assimilabili. L’Unione, in qualità di Titolare del trattamento, deve valutare se attribuire la funzione di amministratore di sistema (o altre funzioni tecniche ad esso assimilabile) e le modalità di svolgimento dell'incarico, insieme alle qualità tecniche, professionali e di condotta del soggetto individuato. Tali valutazioni vanno inquadrate anche alla luce delle responsabilità, di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare da incauta o inidonea designazione.

Infine, l’Unione deve adottare o aggiornare le misure di sicurezza che il Codice Privacy prevede al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

6

Le misure di sicurezza per il trattamento dei dati nel modello associato

Il Titolare custodisce i dati personali trattati nell'ambito della gestione tributaria in modo da ridurre al minimo 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.

La prevenzione ed il controllo di questi rischi sono effettuati mediante l'adozione di misure di sicurezza minime e idonee. Le misure minime, obbligatorie, sono individuate dal Codice e il Disciplinare tecnico (allegato "B" del Codice, aggiornato dal legislatore) ne definisce le modalità di attuazione per i trattamenti elettronici e non. Le misure idonee sono definite dal Titolare in relazione alla natura dei dati, al progresso tecnico e alle caratteristiche del trattamento.

Di seguito si trova una tabella che raccoglie, illustrandole dettagliatamente, le misure di minime sicurezza. Tali misure sono distinte in relazione ai trattamenti effettuati con l'ausilio di strumenti elettronici e senza l'ausilio di strumenti elettronici, e vengono ricondotte ai di-

versi punti e sezioni in cui si articola l'allegato "B. Disciplinare tecnico in materia di misure minime di sicurezza" al Codice Privacy.

Rif. all. B Disciplinare Tecnico	Misure minime di sicurezza Trattamenti effettuati con l'ausilio di strumenti elettronici	Unione di comuni	Singolo comune aderente
Sistema di autenticazione informatica			
p.to n° 2	Assegnazione ad ogni incaricato di una o più credenziali di autenticazione che consenta il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti	x	
p.to n° 2	Credenziali di autenticazione conosciute solo dall'incaricato e ad esso univocamente correlate	x	
p.to n° 7	Disattivazione delle credenziali di autenticazione non utilizzate da almeno 6 mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (es utilizzate dagli amministratori di sistema)	x	x
p.to n° 8	Disattivazione delle credenziali nel caso in cui l'incaricato perda la qualità (ruolo/compito) per l'accesso ai dati personali	x	x
p.to n° 5	Parola chiave, quando prevista dal sistema di autenticazione, composta da almeno 8 caratteri	x	
p.to n° 5	Parola chiave composta da un numero di caratteri pari al massimo consentito (nel caso in cui lo strumento elettronico non permetta la creazione di password di 8 caratteri)	x	
p.to n° 5	Modifica della parola chiave da parte degli Incaricati al primo utilizzo	x	
p.to n° 5	Modifica della parola chiave, nel caso di trattamenti di dati comuni, da parte degli Incaricati almeno ogni 6 mesi	x	
p.to n° 5	Modifica della parola chiave, nel caso di trattamento di dati sensibili e di dati giudiziari, almeno ogni 3 mesi	x	
p.to n°6	Codice per l'identificazione, laddove usato, non è assegnato ad altri incaricati, neppure in tempi diversi	x	x
Sistema di autorizzazione			
p.to n° 12	Sistema di autorizzazione nel caso in cui siano previsti per gli incaricati più profili di autorizzazione con ambiti diversi	x	x
p.to n° 13	Individuazione e configurazione prima dell'inizio del trattamento dei profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati	x	
p.to n° 14	Verifica periodica (almeno annuale) della sussistenza delle condizioni per la conservazione dei profili di autorizzazione	x	x

Altre misure di sicurezza			
p.to n°16	Implementazione di strumenti elettronici per garantire la protezione dei dati personali contro il rischio di intrusione (Firewall) e dell'azione di virus o software dannosi (Antivirus)	x	
p.to n°16	Aggiornamento di tali strumenti con cadenza almeno semestrale	x	
p.to n°17	Aggiornamento dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (es. SERVICE PACK E PATCHES) almeno annuale	x	
p.to n°17	Aggiornamento di questi sw, in caso di trattamento di dati sensibili o giudiziari, almeno semestrale	x	
Ulteriori misure in caso di trattamento di dai sensibili e giudiziari			
p.to n°24	I dati idonei a rilevare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche dati attraverso l'ausilio di strumenti elettronici, sono trattati, con tecniche di cifratura o mediante altre soluzioni che rendano i dati temporaneamente inintelligibili anche a chi è autorizzato ad accedervi permettono di identificare gli interessati solo in caso di necessità e comunque soluzioni che permettano di trattare questi dati sensibili separatamente dai dati personali che permettono di identificare direttamente l'interessato		
Sistema di autenticazione informatica			
p.to n° 4	Redazione di specifiche istruzioni scritte rilasciate agli incaricati, in cui è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale (password)	x	
p.to n° 5	Formalizzazione del divieto di comporre la parola chiave con riferimenti agevolmente riconducibili all'incaricato (es. nome, data di nascita, nomi di familiari)	x	
p.to n° 9	Redazione di specifiche istruzioni scritte rilasciate agli incaricati in cui è prescritto di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento	x	
p.to n° 10	Redazione di disposizioni che individuano le modalità con le quali il Titolare può assicurare, in caso di necessità operativa, la disponibilità dei dati o degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato	x	
p.to n° 10	Individuazione per iscritto dei soggetti incaricati della custodia delle credenziali di autenticazione nel caso in cui sia tecnicamente impossibile garantire l'accesso ai dati senza l'utilizzo della componente riservata delle credenziali di autenticazione (password)	x	
p.to n° 10	Redazione di procedure che disciplinino la custodia delle copie delle credenziali garantendo la massima segretezza	x	
p.to n° 10	Redazione di procedure che disciplinano le modalità operative per informare tempestivamente l'incaricato circa l'utilizzo della propria credenziale di autenticazione per l'accesso al sistema in sua assenza	x	

Altre misure di sicurezza			
p.to n° 15	Aggiornamento periodico (almeno annualmente) della lista degli incaricati e degli addetti alla gestione/manutenzione degli strumenti elettronici e del relativo ambito del trattamento dei dati personali	x	x
p.to n° 18	Redazione di istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale	x	
Documento Programmatico sulla Sicurezza			
p.to n° 19	Redazione del Documento Programmatico sulla Sicurezza nell'ipotesi di trattamenti di dati sensibili e giudiziari	x	
p.to n° 19	Aggiornamento del documento entro il 31 marzo di ogni anno	x	x
p.to n° 19	Analisi dei rischi	x	x
p.to n° 19	Piano di formazione per gli incaricati	x	x
p.to n° 19	Adozione di criteri per garantire l'adozione di misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare (OUTSOURCING)	x	
Ulteriori misure in caso di trattamento di dati sensibili e giudiziari			
p.to n° 21	Redazione di istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati (sensibili e giudiziari) al fine di evitare accessi non autorizzati e trattamenti non consentiti		
p.to n° 22	I supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, sono distrutti o resi inutilizzabili		
p.to n° 22	I supporti rimovibili contenenti dati sensibili o giudiziari vengono riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, esclusivamente nell'ipotesi in cui le informazioni non siano intelligibili e tecnicamente in alcun modo recuperabili		
p.to n° 23	Adozione di idonee misure e specifiche procedure per garantire il ripristino dell'accesso ai dati (sensibili e giudiziari) in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati (max 7gg)		
p.to n° 24	Trattamento dati relativi all'identità genetica		
Misure di tutela e garanzia			
p.to n° 25	Qualora ci si avvalga di soggetti esterni alla propria struttura per adottare misure minime di sicurezza si richiede all'installatore una descrizione scritta dell'intervento effettuato che n' attesta la conformità alle disposizioni del presente disciplinare	x	
p.to n° 26	Nella relazione accompagnatoria del bilancio (se dovuta), il titolare riferisce l'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza	x	x

Rif. all. B Disciplinare Tecnico	Misure minime di sicurezza Trattamenti effettuati senza l'ausilio di strumenti elettronici		
p.to n° 29	Accesso controllato agli archivi contenenti dati sensibili o giudiziari		
p.to n° 29	Accesso dopo l'orario di chiusura agli archivi contenenti dati personali o sensibili	x	
p.to n° 29	Le persone ammesse, agli archivi contenenti dati sensibili e giudiziari, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate		
p.to n° 29	Quando gli archivi, contenenti dati sensibili e giudiziari, non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate		
p.to n° 27	Esistenza di specifiche istruzioni scritte rilasciate agli incaricati finalizzate al controllo e alla custodia degli atti e dei documenti contenenti dati personali, per l'intero ciclo necessario allo svolgimento dei propri compiti		
p.to n° 27	Aggiornamento periodico (almeno annuale) della lista degli incaricati e del relativo ambito del trattamento dei dati personali	x	x
p.to n° 28	Gli Incaricati del trattamento cui sono affidati di atti e documenti contenenti dati sensibili o giudiziari prestano un costante presidio sugli stessi (i medesimi atti e documenti sono controllati e custoditi dagli stessi incaricati fino alla restituzione in modo che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate)		

7

Fasi di aggiornamento del “sistema privacy”

(per le attività di gestione tributaria)

Di seguito si riassumono le fasi che caratterizzano il processo di adeguamento del “sistema Privacy” dell’Unione e dei singoli comuni aderenti, a seguito dell’attivazione del sistema di gestione tributaria in forma associata.

L’obiettivo è quello di suggerire un percorso utile per mettere in condizione l’Unione e i singoli comuni aderenti di tutelare gli interessi dei soggetti pubblici e privati che fanno affidamento sui trattamenti svolti dagli Enti, riducendo il rischio di eventi pregiudizievoli che possano danneggiare disponibilità, riservatezza e integrità del patrimonio di dati degli Enti.

La consapevolezza che rischi e insidie possono coinvolgere l’utilizzo dei sistemi informativi automatizzati e gli archivi cartacei, rende inevitabile la ricerca di possibili soluzioni tecnico/organizzative per prevenire situazioni di pericolo per le risorse e per chi se ne avvale, nonché per affrontare e risolvere eventuali problemi derivanti dal verificarsi di eventi lesivi del patrimonio informativo.

In corrispondenza delle differenti fasi, nella colonna “Attività” vengono descritte le attività che l’Unione e i singoli comuni aderenti devono svolgere al fine di adeguare il proprio “sistema Privacy” al nuovo assetto organizzativo. Nella successiva colonna “Finalità” vengono definite le finalità delle azioni che l’Unione e i singoli comuni aderenti devono intraprendere. Nell’ultima colonna viene indicata il riferimento alla scheda elaborata, descritta nel paragrafo successivo.

Fase	Attività	Finalità	Rif. Scheda
1	mappatura delle banche dati e dei trattamenti di dati personali, suddividendoli tra dati trattati con l’ausilio di strumenti elettronici e dati trattati senza l’ausilio di strumenti elettronici	rilevare le banche dati, la loro collocazione e i trattamenti effettuati, i soggetti che effettuano in trattamenti	Scheda 1
2	analisi del livello di applicazione delle misure per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità	verificare il grado di applicazione delle misure minime di sicurezza di cui all’allegato B Disciplinare Tecnico	Scheda 2
3	rilevazione dei rischi che incombono sui dati e definizione di un piano di adeguamento	analizzare i rischi che incombono sui dati	Scheda 3
		implementare il livello di applicazione delle misure per: <u>Trattamenti con l’ausilio di strumenti elettronici</u> - Sistema di autenticazione informatica - Sistema di autorizzazione - Altre misure di sicurezza - Documento Programmatico sulla Sicurezza - Misure di tutela e garanzia <u>Trattamenti senza l’ausilio di strumenti elettronici</u>	
4	esame della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati	valutare l’individuazione della figura di Amministratore di sistema (o equivalente)	Scheda 4
		valutare l’individuazione della figura di responsabile (eventualmente in outsourcing)	Scheda 5
		verificare / aggiornare l’ambito di trattamento dati degli incaricati,	Scheda 6

8

Schede standard per realizzare le fasi

Nel presente paragrafo si presentano, in formato di schede operative elaborate in versione standard, i modelli utili per l'adeguamento del "sistema Privacy" a seguito dell'attivazione del sistema di gestione tributaria in forma associata. Tali modelli "prototipali" consentono di rilevare in modo standardizzato e organico, all'interno dell'Unione e dei comuni aderenti, lo stato dell'arte relativo all'adozione delle disposizioni in materia di protezione dei dati personali e di accompagnare gli adeguamenti necessari.

Di seguito si illustrano le schede allegate.

- SCHEDA 1 - ALLEGATO 1
- SCHEDA 2 - ALLEGATO 2
- SCHEDA 3 - ALLEGATO 3
- SCHEDA 4 - ALLEGATO 4
- SCHEDA 5 - ALLEGATO 5
- SCHEDA 6 - ALLEGATO 6

8.1 Scheda 1

Si articola in quattro sezioni:

- MAPPATURA ARCHIVI: per ogni archivio trattato, consente di rilevare i tipi di dati oggetto di trattamento, le modalità di trattamento e i soggetti autorizzati al loro trattamento
- ARCHITETTURA SISTEMA (ambiente operativo): per ogni archivio trattato a livello informatico, consente di rilevare sinteticamente i principali requisiti dell'ambiente operativo e le sue principali caratteristiche di sicurezza
- ARCHITETTURA SISTEMA (applicativo): per ogni archivio trattato a livello informatico, consente di rilevare i requisiti del sistema applicativo che ne tratta i dati contenuti
- ARCHITETTURA SISTEMA (manutenzione): per ogni archivio trattato a livello informatico, consente di rilevare i requisiti di manutenzione

N.B.: per ogni archivio (e relativo software) utilizzare una nuova riga. Compilare, se possibile, tutte le celle della riga stessa. Non usare righe diverse per lo stesso software. Non sono da considerare i software come Word, Excel. Archivi strutturati fatti con Access invece sono da prendere in considerazione. File salvati sui dischi condivisi ("Zone Centrali") non devono essere presi in considerazione. Se su tali "zone" sono stati installati degli applicativi allora occorre prenderli in considerazione. Non prendere in considerazione quegli applicativi la cui manutenzione è in carico al Ced (si occupano loro del censimento).

8.2 Scheda 2

Si articola in quattro sezioni:

- SICUREZZA DELL'INFORMAZIONE: consente di rilevare il livello di adozione di alcune misure di sicurezza previste dal "Disciplinare tecnico in materia di misure minime di sicurezza" per i trattamenti di dati con strumenti elettronici
- SICUREZZA FISICA E AMBIENTALE: supporta la rilevazione del grado di sicurezza relativo alle caratteristiche fisiche e ambientali dei componenti del sistema informativo destinato al trattamento di dati
- SISTEMA AUTENTICAZIONE E AUTORIZZAZIONE: consente di rilevare il livello di applicazione di alcune misure di sicurezza previste dal "Disciplinare tecnico in materia di misure minime di sicurezza" per i trattamenti di dati con strumenti elettronici

8.3 Scheda 3

È dedicata alla rilevazione del profilo di rischio connesso al trattamento dei dati. Vengono individuate tre principali macroaree di rischio (sottrazione credenziali, eventi legati agli strumenti elettronici ed eventi legati al contesto) che possono essere ulteriormente personalizzate. Le tre macro aree vengono declinate in un elenco di tipologie di rischi per ognuna delle quali si chiede di valutare, motivandolo, il grado di rischio e l'impatto (gravità) sul trattamento dei dati nel caso in cui l'evento rischioso si realizzi. Nell'ultima colonna è possibile inserire le eventuali azioni da intraprendere per ridurre e controllare specifiche tipologie di rischio.

8.4 Scheda 4

Contiene una bozza utile per la formalizzazione delle funzioni e delle responsabilità della figura di Amministratore di sistema/database/rete/… Tale bozza, che si sviluppa sulla base dei contenuti del provvedimento del 27 novembre 2008 del Garante Privacy, può essere utilizzata nei casi in cui la figura è interna all'organizzazione del titolare ed è già stata individuata come incaricata di specifici trattamenti di dati.

8.5 Scheda 5

Contiene una bozza utile per la formalizzazione delle funzioni e delle responsabilità attribuibili alla figura di Responsabile (esterno) per il trattamento dei dati. Responsabile è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. La designazione formale di tale figura è facoltativa. Tale bozza può essere utilizzata nei casi in cui i trattamenti di dati personali sono affidati, in conformità al codice, all'esterno della struttura del Titolare. In ogni caso, il Documento Programmatico della Sicurezza (cfr. 19.7 Allegato B al Codice Privacy) deve contenere la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.

8.6 Scheda 6

Contiene una bozza utile per la formalizzazione delle funzioni e delle responsabilità della figura di Incaricato al trattamento. Gli incaricati sono le persone fisiche autorizzate a com-

piere operazioni di trattamento dal Titolare (e/o dal Responsabile, se designato), operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite e la designazione (effettuata in forma scritta) individua puntualmente l'ambito del trattamento consentito. Le misure minime di sicurezza dispongono l'obbligo di aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati. Tale bozza contiene anche una sintesi generale di possibili istruzioni operative da assegnare agli incaricati

Allegati

Scheda 1

Scheda 2

Scheda 3

Scheda 4

Scheda 5

Scheda 6

Scheda 1

1a. MAPPATURA ARCHIVI											
N°	**archivio / data base** (e relative finalità di trattamento)	**Dati "comuni"**	**Dati sensibili**	**Dati giudiziari**	**ELABORAZIONE cartacea**	**ELABORAZIONE informatica**	**ARCHIVIO cartaceo**	**ARCHIVIO informatico**	**Responsabile del trattamento** (eventuale)	**Elenco incaricati**	**Note** (indicare il relativo numero di colonna per il quale si desidera inserire delle note)
1	*ESEMPIO:* data base scia	elencare tipo di dati	elencare tipo di dati	elencare tipo di dati	si/no	si/no	si/no; ubicazione	si/no; indicare se data base locale/centrale;			
2											

1b. ARCHITETTURA DEL SISTEMA (ambiente)								
Server: denominazione hardware	**Server: sistema operativo**	**vengono utilizzati programmi antivirus automatici**	**N° PC collegati in rete**	**ubicazione**	**N° PC standalone**	**ubicazione**	**Manutenzione hardware**	**Note** (indicare il relativo numero di colonna per il quale si desidera inserire delle note)
		si/no					si/no	

1c. ARCHITETTURA DEL SISTEMA (applicativo)								
Nome applicativo	**Descrizione**	**Versione**	**Produttore**	**Tipologia (gestionale o specifico)**	**tratta dati personali**	**tratta dati giudiziari**	**tratta dati sensibili**	**Note** (indicare il relativo numero di colonna per il quale si desidera inserire delle note)
					si/no	si/no	si/no	

1d. ARCHITETTURA DEL SISTEMA (manutenzione)						
Manutenzione software	**Società incaricata per la manutenzione**	**Data ultimo aggiornamento**	**Data ultimo intervento dell'assistenza**	**Tempestività media degli interventi d'assistenza (giorni)**	**Modalità d'intervento (remota o in loco)**	**Note** (indicare il relativo numero di colonna per il quale si desidera inserire delle note)
si/no						

Scheda 2

2a. SICUREZZA DELL'INFORMAZIONE											
Eventuali PC non in rete: vengono utilizzati programmi antivirus	**Questi programmi sono aggiornati con cadenza almeno annuale**	**Sono definite le responsabilità, a livello di procedura, di chi deve garantire la salvaguardia di ogni componente del sistema informativo**	**Viene effettuato periodicamente una verifica dei processi atti a garantire la sicurezza dell'informazione**	**Il personale che utilizza il sistema informativo è stato formato al fine della salvaguardia della sicurezza dell'informazione**	**Sono effettuate copie di back-up con periodicità almeno settimanale**	**Le copie di back-up sono custodite in luogo sicuro**	**Esiste una procedura per il back-up dei dati dei PC standalone**	**Esiste un piano di Disaster Recovery per il ripristino del sistema**	**Si ha un aggiornamento, o patch, almeno semestrale dei programmi volta a prevenire la vulnerabilità dei sistemi elettronici e correggerne i difetti**	**Sono definite le modalità di trattamento dei supporti informatici removibili**	**Note** (indicare il relativo numero di colonna per il quale si desidera inserire delle note)
si/no; indicare quali	si/no; indicare periodicità aggiornamento	si/no	si/no	si/no	si/no; indicare periodicità	si/no	si/no	si/no	si/no	si/no	

2b. SICUREZZA FISICA ED AMBIENTALE				
I componenti del sistema informativo sono in locali protetti e con controllo degli accessi	**Le linee di comunicazione utilizzate dalle banche dati classificate sono adeguatamente protette**	**Le dismissioni di banche dati classificate sono autorizzate in modo adeguato**	**L'accesso al CED/Server è controllato e limitato agli addetti**	**Note** (indicare il relativo numero di colonna per il quale si desidera inserire delle note)
si/no	si/no	si/no	si/no	

2c. SISTEMA AUTENTICAZIONE ED AUTORIZZAZIONE															
Per l'accesso è attribuito un Codice Identificativo Personale	**Esiste una procedura per disattivare Il Codice Identificativo Personale se non più necessario**	**Esiste una procedura volta a consentire la disattivazione del Codice Identificativo Personale in caso di mancato utilizzo per 6 mesi**	**Esiste una Password per ogni incaricato al trattamento dei dati sensibili**	**La Password è composta da almeno 8 caratteri**	**La Password viene cambiata almeno ogni 6 mesi**	**La Password viene modificata in autonomia dall'incaricato**	**Esiste una procedura per consentire accesso in caso di assenza dell'incaricato**	**Sono stati individuati i diversi Profili di Autorizzazione per l'accesso ai dati sensibili**	**Sono individuati profili di autorizzazione anteriori al trattamento**	**E' stato designato in forma scritta il responsabile del trattamento dei dati personali**	**E' stato designato in forma scritta l'icaricato per il trattamento dei dati personali**	**E' verificato che uno stesso codice identificativo non sia assegnato a diversi incaricati, neppure in tempi diversi**	**Almeno annualmente vengono verificati i Profili di Autorizzazione**	**Vi sono istruzioni scritte per gli incaricati, relativamente alla diligente custodia delle password**	**Note** (indicare il relativo numero di colonna per il quale si desidera inserire delle note)
si/no	si/no	si/no	si/no	si/no	si/no	si/no	si/no	si/no	si/no	si/no	si/no	si/no	si/no	si/no	

Scheda 3

RISCHI 1-sottrazione di credenziali 2-eventi relativi agli strumenti 3-eventi relativi al contesto	TIPOLOGIA DI RISCHIO	GRADO RISCHIO P=presente A=assente N/A=non applic	IMPATTO (BASSO/MEDIO/ALTO)	MOTIVAZIONE DEL LIVELLO DI RISCHIO	PIANO DI ADEGUAMENTO
1 - sottrazione di credenziali di autenticazione	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
1 - carenza di consapevolezza, disattenzione o incuria	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
1 - comportamenti sleali o fraudolenti	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				

	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
1- errore materiale	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
2 - azione di virus o programmi potenzialmente dannosi	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
2 - spamming o tecniche di sabotaggio	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				

	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
2 - malfunzionamento, indisponibilità o degrado degli strumenti	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
2 - accessi esterni non autorizzati a locali/aree	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
2 - intercettazione di informazioni in rete	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				

	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
3 - ingressi non autorizzati a locali/aree ad accesso ristretto	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
3 -sottrazione di strumenti contenenti dati	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
3 - eventi distruttivi naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				

	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				
3 - guasto a sistemi complementari (impianto elettrico, climatizzazione,…)	Rischi sugli aspetti organizzativi e normativi				
	Rischi sui luoghi fisici				
	Rischi sulle risorse hardware				
	Rischi sulle risorse software				
	Rischi sulle risorse dati				

Scheda 4

Designazione di amministratore di sistema (interno)

Provv. 27.11.2008 Garante Privacy

Gentile Signora/ Egregio Signore (inserire nome e cognome)

il D. lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) sancisce che "chiunque ha diritto alla protezione dei dati personali che lo riguardano" e individua una serie di garanzie e principi per assicurare il rispetto dei diritti e delle libertà fondamentali, la riservatezza, l'identità personale e il diritto alla protezione dei dati.

In ottemperanza a quanto previsto dal Codice della Privacy, Lei è già stato designato quale incaricato del trattamento dei dati: tale designazione rende legittime le operazioni di trattamento da Lei effettuate.

Con provvedimento del 27 novembre 2008 (pubblicato in G.U. n. 300 del 24/12/2008), il Garante della Privacy ha prescritto di individuare e designare gli amministratori di sistema. Valutati i suoi requisiti di esperienza, capacità e affidabilità, nell'ambito delle funzioni da Lei già svolte in qualità di incaricato del trattamento con accesso privilegiato ai dati, Xxxxxxx con sede in Xxxxxxx via Xxxxxxx n. xx, "**Titolare del trattamento**", rappresentata da Xxxxxxx Xxxxxxx nato a Xxxxxxx il xx.xx.19xx in qualità di legale rappresentante pro-tempore La designa formalmente **amministratore di sistema**.

In particolare Lei opera come (indicare una o più figure di amministratore di sistema tra le seguenti: **Amministratore di network; Amministratori di Unità elaborative (Mainframe, Server); Amministratori di banche dati; Amministratori delle applicazioni; Amministratori di backup/restore**) e come tale è addetto alle seguenti attività: (selezionare tutte le attività relative alla/alle figura/e di amministratore di sistema ricoperta/e)

Amministratore di network – attività:

- operare sull'infrastruttura di rete gestendo gli apparati e i dispositivi di rete, creando e modificando le regole di funzionamento
- operare nella gestione logica eseguendo operazioni sui "servizi di directory" e sui relativi protocolli. Per le reti Microsoft, nell'ambito dei servizi di directory, sono da considerare amministratori di sistema gli amministratori dei domini (compresi i child) e coloro i quali gestiscono i differenti protocolli applicativi (LDAP1, DNS2, DHCP3, SMTP4, RAS5, ecc.). Sono altresì da considerare come amministratori di sistema anche gli amministratori di VPN utilizzate

Amministratori di Unità elaborative (Mainframe, Server) – attività:

- configurazione dei sistemi operativi e modifica delle impostazioni;
- accesso completo al file system;
- condivisione con altri utenti delle risorse presenti sull'unità elaborativa e sui dispositivi di memorizzazione di massa;
- aggiornamento dei sistemi a garanzia della sicurezza e del buon andamento dei sistemi stessi (patch, fix ecc.);
- accesso ai file di configurazione oppure ai registri delle unità elaborative;
- attribuzione ad altri utenti dei privilegi per l'accesso alle unità elaborative;
- possibilità di configurare le policy locali del sistema operativo;
- esecuzione in modalità batch oppure interattiva di comandi o di sequenze di comandi (scripts).

Amministratore di banche dati – attività:

- creare, modificare oppure eliminare le "strutture" atte a contenere i dati oggetto del trattamento;
- effettuare interrogazioni, anche complesse, puntuali o massive sulla banca dati (es. utilizzo di SQL negli RDBMS);
- esportare insiemi o sottoinsiemi di dati in formato standard o proprietario;
- assegnare, modificare, limitare e/o escludere l'accesso ai dati da parte di ogni singolo utente;
- eseguire comandi o sequenze di comandi (script) in modalità interattiva oppure batch che permettono la modifica massiva della banca dati;
- rendere disponibili/indisponibili le "strutture" che contengono dati.

Amministratori delle applicazioni – attività:

- creare/modificare/eliminare gli altri utenti degli applicativi (es. modifica credenziali d'accesso);
- effettuare attraverso l'applicazione modifiche o interrogazioni massive.

Amministratori di backup/restore – attività:

- eseguire le operazioni di salvataggio e ripristino delle banche dati e delle "strutture" che le ospitano

Nella Sua funzione di amministratore di sistema Lei dovrà attenersi ai doveri di lealtà, correttezza, imparzialità, onestà e diligenza, utilizzando gli strumenti informatici esclusivamente per l'adempimento delle attività inerenti al Suo ambito di lavoro.

Si precisa che, in osservanza del citato provvedimento del Garante, gli accessi logici agli strumenti informatici, ai sistemi di elaborazione e agli archivi elettronici, di cui Lei è amministratore saranno oggetto di registrazione e conservazione per almeno sei mesi. Inoltre si prevedono controlli periodici, con frequenza almeno annuale, sull'operato degli amministratori di sistema, al fine di controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto al trattamento dei dati personali previste dalle norme vigenti.

Considerato che Lei riveste la qualità di amministratore di sistema incaricato di attività inerenti al trattamento dei dati di cui è **Titolare** il **Yyyyyyyyyy**, in base a quanto prescritto dal provvedimento del Garante il Suo nominativo sarà reso noto a **Yyyyyyyyyy**. (N.B.: Quest'ultimo punto è da inserire soltanto nella nomina di quegli amministratori di sistema effettivamente preposti a svolgere attività che riguardino direttamente od indirettamente il trattamento di dati di cui rimane Titolare **Yyyyyyyyyy**)

Considerato che Lei riveste la qualità di amministratore di sistema incaricato di attività inerenti al trattamento dei dati di dipendenti di Xxxxxxx, in base a quanto prescritto dal provvedimento del Garante il Suo nominativo sarà reso noto ai dipendenti stessi ai sensi dell'art. 13 del Codice della Privacy. (N.B.: Quest'ultimo punto è da inserire soltanto nella nomina di quegli amministratori di sistema effettivamente preposti a svolgere attività che riguardino direttamente od indirettamente il trattamento di informazioni di carattere personale dei dipendenti del Xxxxxxx)

Si ricorda infine che l'inosservanza delle disposizioni in materia di trattamento dei dati ed il comportamento non conforme alla funzione svolta può determinare effetti pregiudizievoli per il Titolare e comportare responsabilità dirette e personali.

Xxxxxxx, _____

Il Titolare o Responsabile del trattamento

Xxxxxxx

Rappresentato da:

Xxxxxxx Xxxxxxx

Firma per ricevuta:

Scheda 5

Designazione del Responsabile del Trattamento dei dati personali

D.Lgs. 196/03

Ai sensi dell'art. 29 del D. Lgs. 30 giugno 2003 n. 196 "Codice in materia dei dati personali" (di seguito Codice) il **Xxxxxxxxxxxxxxx**, in qualità di "**Titolare del trattamento**", rappresentato da (**INSERIRE IL SOGGETTO CHE RAPPRESENTA IL Xxxxxxxxxxx**), con sede in **Xxxxxxxxxxx**, via **Xxxxxxxxxxx** n. _____ designa **Yyyyyyyyyy**, in persona del legale rappresentante pro tempore **INSERIRE IL SOGGETTO CHE RAPPRESENTA Yyyyyyyyyy**, con sede in **Yyyyyyyyyy** via **Yyyyyyyyyy** n. _____, quale "**Responsabile**" per il trattamento dei dati personali per l'esecuzione delle attività previste dal contratto/convenzione "**Xxxxxxxxxxx Xxxxxxxxxxx Xxxxxxxxxxx Xxxxxxxxxxx**" sottoscritto in data ___ / ___ / ___ prot. _____/201_.

1. Requisiti di professionalità.
Il Responsabile designato è dotato di requisiti di esperienza, capacità ed affidabilità tali da fornire idonea garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, compreso il profilo relativo alla sicurezza.

2. Ambito e limiti del trattamento dei dati
Il Responsabile è autorizzato ad effettuare esclusivamente le operazioni di trattamento necessarie per lo svolgimento del servizio affidato: **Xxxxxxxxxxx Xxxxxxxxxxx Xxxxxxxxxxx Xxxxxxxxxxx**. Il Responsabile riconosce che le finalità del trattamento sono esclusivamente quelle individuate nel contratto sottoscritto tra le parti in data ___ / ___ / ___ o quelle successivamente concordate.

3. Compiti e dichiarazioni del Responsabile
3.1. Il Responsabile nell'espletamento della propria funzione deve attenersi agli obblighi posti dal Codice e deve collaborare con il Titolare, fornendo le informazioni e i documenti richiesti, ed eventuali relazioni sullo stato di attuazione della normativa, sul modello organizzativo adottato e su certificazioni di sicurezza acquisite. In tale ambito il Titolare si riserva la facoltà di visionare e/o estrarre copia del DPS del Responsabile.
3.2. Il Responsabile si impegna altresì a rispettare in ogni fase del trattamento le disposizioni previste dal Codice, in particolare le finalità, le modalità, le misure di sicurezza e gli ambiti di comunicazione dei trattamenti.
3.3. Fermo restando quanto previsto ai precedenti punti 3.1 e 3.2, il Responsabile dichiara di aver ricevuto, esaminato, condiviso e compreso le istruzioni impartite dal Titolare con i documenti contrattuali, nonché quelle di seguito indicate alle quali dovrà attenersi nell'esecuzione dell'incarico.
4. Istruzioni per il Responsabile.
4.1 Il Responsabile nell'esercizio delle proprie funzioni:

- garantisce che i dati personali oggetto di trattamento sono controllati e custoditi, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento stesso;
- attua a tal fine tutte le misure, anche organizzative e logistiche, finalizzate alla custodia e al controllo dei dati, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, nonché di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta; a tal riguardo il Responsabile fornisce la documentazione relativa al piano di sicurezza del data center, che descrive le misure di sicurezza adottate in rapporto al servizio oggetto della presente designazione;
- cura in caso di trattamento con strumenti elettronici il corretto adempimento degli obblighi di cui all'art 34 del Codice, secondo cui il trattamento dei dati personali effettuato con tali strumenti è consentito solo se sono adottate tutte le misure di sicurezza indicate nell'allegato B del Codice;
- adotta pertanto le misure di sicurezza contenute negli articoli da 31 a 36 del Codice stesso e nel Disciplinare Tecnico (Allegato B al citato Codice);
- non comunica a terzi né diffonde i dati di cui viene a conoscenza, salvo che tali operazioni siano autorizzate dal Titolare del trattamento e previste da norme di legge o di regolamento;
- redige l'informativa ai sensi dell'art. 13 del Codice e la sottopone al Titolare per l'approvazione e anche per concordare le modalità con cui fornirla agli interessati;
- non effettua di propria iniziativa alcuna operazione di trattamento diversa da quelle previste se non autorizzata dal Titolare;
- garantisce al Titolare - se da questo richiesto - la tutela dei diritti innanzi al Garante per la protezione dei dai personali in caso di eventuali contenziosi rispetto al servizio offerto;
- realizza tutto quanto sia utile e/o necessario per garantire gli adempimenti di tutti gli obblighi previsti dal Codice.
-

4.2 Il Titolare, in funzione di eventuali evoluzioni tecnologiche e/o normative, può richiedere ulteriori misure di sicurezza rispetto a quelle minime adottate e diverse da quelle stabilite dal Responsabile per il trattamento. In tal caso il Titolare fornirà al Responsabile adeguate istruzioni con sufficiente preavviso per permettere allo stesso di attuarle.
Il Responsabile, al termine delle attività connesse alla funzione e delle prestazioni contrattualmente previste:

- consegna al Titolare tutte le informazioni raccolte, nel formato in cui esse si trovano (cartaceo e/o elettronico);
- consegna al Titolare i supporti rimovibili eventualmente utilizzati in cui sono memorizzati i dati.

Il Responsabile inoltre, fermo restando l'impegno di cui al punto 4.1 penultimo capoverso, distrugge tutte le informazioni registrate su supporto fisso documentando per iscritto l'adempimento di tale operazione.

5. Incaricati del trattamento.
Il Responsabile individua e designa i propri "Incaricati" del Trattamento fornendo loro, per iscritto, le istruzioni in merito ai trattamenti secondo quanto previsto dal Codice, con particolare riferimento alle indicazioni relative alle operazioni che possono essere svolte sui dati.
Il Responsabile sottopone gli incaricati ad interventi formativi e di aggiornamento periodico o approfondimento per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure adottate.

Gli incaricati hanno accesso ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati, e possono compiere i soli trattamenti individuati con riferimento alle finalità connesse alla funzione e delle prestazioni contrattualmente previste.
Il Responsabile avrà cura di fornire agli Incaricati che, per mansioni e funzioni, avranno accesso ai dati personali comuni, sensibili e giudiziari tutte le indicazioni e le specifiche regole comportamentali affinché i trattamenti effettuati siano conformi ai principi di pertinenza, non eccedenza e indispensabilità.

6. Amministratori di sistema
Il Responsabile comunica i nominativi degli amministratori di sistema, preventivamente individuati e designati secondo le modalità e le indicazioni fornite dall'Autorità Garante per la protezione dei dati personali con provvedimento del 27 novembre 2008 (pubblicato in G.U. n. 300 del 24/12/2008) e successive modifiche.

7. Responsabilità
Il Responsabile risponde ai sensi dell'art. 2049 c.c. per qualsiasi danno cagionato al Titolare o a terzi derivante da atti, fatti o omissioni posti in essere in violazione delle disposizioni del Codice in materia di protezione dei dati personali, anche dai propri incaricati del trattamento e dagli amministratori di sistema.

8. Dichiarazioni e compiti del Titolare
Il Titolare precisa che i dati personali dovranno essere raccolti e conservati dal Responsabile nel rispetto delle disposizioni di legge ed in particolare del Codice; i dati dovranno essere esatti ed aggiornati, pertinenti, completi e non eccedenti le finalità per le quali sono trattati.
Il Titolare, nell'esercizio delle proprie funzioni, vigila sulla puntuale osservanza delle disposizioni previste dal Codice, con particolare riguardo alle misure di sicurezza adottate dal Responsabile anche con verifiche periodiche. A tal fine ne dà comunicazione al Responsabile del trattamento dei dati con un preavviso minimo di tre giorni lavorativi

9. Rapporti con il Garante
Ciascun soggetto (Titolare e Responsabile) informerà l'altro tempestivamente di ogni provvedimento del Garante in relazione ai Trattamenti dei dati oggetto delle attività previste dal "**Xxxxxxxxxxx Xxxxxxxxxxx Xxxxxxxxxxx Xxxxxxxxxxx**" sottoscritto in data ___ / ___ / ___ prot. _____/201_. In particolare il Responsabile avvisa immediatamente il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante.

10. Rapporti con gli interessati (ex art. 7 del D. Lgs. 196/03).
Ciascun soggetto (Titolare e Responsabile) informerà l'altro tempestivamente in ordine alle richieste prodotte ai sensi dell'articolo 7 del Codice da parte degli interessati.
Su richiesta del Titolare, il Responsabile fornisce riscontro alle eventuali istanze degli interessati nei termini previsti dal Codice. Il Responsabile, prima di provvedere, sottopone al Titolare la risposta che intende fornire in merito al trattamento dei dati.

11. Corrispettivo e spese
Nessun corrispettivo è dovuto dal Titolare al Responsabile per l'espletamento della funzione.

12. Cessazione e Revoca
La presente designazione cessa automaticamente alla data di naturale scadenza del Protocollo prevista dall'art. 12 dello stesso. Il Titolare può revocare l'incarico in caso di svolgimento delle

funzioni non conforme alle istruzioni fornite, nonché per la sopravvenuta perdita dei requisiti di cui all'art. 29 del Codice o per esigenze di interesse pubblico.

Xxxxxxxxxxx, _____

Il Titolare del trattamento	**Il Responsabile del Trattamento**
Xxxxxxxxxxx	**Yyyyyyyyyy**
Rappresentato da:	**Rappresentato da:**

Scheda 6

Designazione di incaricato al trattamento dei dati

Gentile Signora/ Egregio Signore (inserire nome e cognome)

il D. lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" (di seguito Codice) sancisce che "chiunque ha diritto alla protezione dei dati personali che lo riguardano" e individua una serie di garanzie e principi per assicurare il rispetto dei diritti e delle libertà fondamentali, la riservatezza, l'identità personale e il diritto alla protezione dei dati.

Ai sensi dell'art. 30 del Codice il Xxxxxxxxxxxxxxx, in qualità di "Titolare del trattamento", rappresentato da (INSERIRE IL SOGGETTO CHE RAPPRESENTA IL Xxxxxxxxxxx), con sede in Xxxxxxxxxxx, via Xxxxxxxxxxx n. _____ designa Yyyyyyyyyy quale "Incaricato" per il trattamento dei dati personali e, in ossequio a dette disposizioni di legge, nello svolgimento delle Sue mansioni potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati.

In particolare Lei tratterà (indicare se con e/o senza strumenti elettronici) i dati personali comuni e/o sensibili e/o giudiziari relativi alle banche dati e per le operazioni indicate di seguito, secondo le sole esigenze dettate dalle Sue mansioni professionali ed in coerenza con il profilo di autorizzazione assegnato:

Banche dati		**Operazioni**
• Qqqqqqq	➔	• Qqqqqqq
• Qqqqqqq	➔	• Qqqqqqq
• Qqqqqqq	➔	• Qqqqqqq
• Qqqqqqq	➔	• Qqqqqqq
• Qqqqqqq	➔	• Qqqqqqq

Nella Sua funzione di incaricato Lei dovrà attenersi ai doveri di lealtà, correttezza, imparzialità, onestà e diligenza, utilizzando gli strumenti informatici esclusivamente per l'adempimento delle attività inerenti al Suo ambito di lavoro.

Inoltre, a seconda che si tratti di operazioni effettuate sui dati con e/o senza strumenti elettronici, in relazione all'Allegato B – Disciplinare tecnico del Codice, dovrà attenersi alle seguenti istruzioni operative:

Trattamenti con strumenti elettronici

- inserire la password richiesta all'avvio del computer. La password è riservata e personale. È composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Non contiene riferimenti agevolmente riconducibili all'incaricato.
- sostituire la password almeno ogni sei mesi (ogni tre mesi nel caso di trattamenti di dati sensibili o giudiziari)
- non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento
- adottare le necessarie cautele per assicurare la segretezza della password e la diligente custodia dei dispositivi in suo possesso (cd, usb memory pen, pc portatili, …)
- quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della password, in caso di prolungata assenza o impedimento dell'incaricato, qualora sia indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, adottare la procedura prevista
- rendere inutilizzabili, mediante cancellazione e formattazione, i supporti rimovibili (floppy disk, cd, usb-memory-pen) contenenti dati sensibili o giudiziari, se non utilizzati. Tali supporti possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Trattamenti senza strumenti elettronici

- controllare e custodire, per l'intera durata delle operazioni di trattamento, gli atti e i documenti contenenti dati personali in maniera che ad essi non accedano persone prive di autorizzazione. In particolare nei periodi in cui la Sua scrivania rimane incustodita durante le operazioni di trattamento, i documenti saranno temporaneamente riposti in cassetti dotati di serratura, tali cassetti dovranno rimanere chiusi e la chiave dovrà rimanere in Suo possesso. Immediatamente dopo il loro utilizzo, i documenti prelevati dovranno essere riposti nell'archivio e gli armadi chiusi a chiave.
- conservare i dati idonei a rilevare lo stato di salute separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. In particolare tali dati sono conservati in fascicoli separati, in un apposito armadio chiuso a chiave.

Si ricorda infine che l'inosservanza delle disposizioni in materia di trattamento dei dati ed il comportamento non conforme alla funzione svolta può determinare effetti pregiudizievoli per il Titolare e comportare responsabilità dirette e personali.

Xxxxxxx, _____

Il Titolare o Responsabile del trattamento

Xxxxxxx

Rappresentato da:
Xxxxxxx Xxxxxxx

Firma per ricevuta:


Progetto
G I T