Comune di Piana degli Albanesi

Provincia di Palermo

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(Approvato con deliberazione del Consiglio Comunale n. 62 del 19/09/2018)

Sommario

Articolo 1 – **Oggetto e finalità**

Il presente Regolamento per il trattamento dei dati personali, in attuazione al Decreto Legislativo n. 196 del 30 giugno 2003, disciplina il trattamento, la comunicazione e la diffusione, da parte del **Comune di Piana degli Albanesi** con sede in Piana degli Albanesi in Via Togliatti, n. 2, dei dati personali contenute nelle banche dati di cui l'ente è Titolare.

L'Ente gestisce le banche dati di cui è titolare, trattati sia con sistemi automatizzati che non automatizzati, nell'ambito del perseguimento dei propri fini istituzionali, nei limiti stabiliti dallo Statuto, dalla legge e dai regolamenti.

Articolo 2 – Definizioni di riferimento

1) Ai fini del presente Regolamento, si applicano le seguenti definizioni elencate nel Decreto Legislativo 196/2003:

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;

incaricati: le persone fisiche autorizzate 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;

informativa: dichiarazione scritta che deve essere resa all'interessato prima di iniziare un'operazione di trattamento di dati che lo riguardano. Contiene, tra le altre cose, l'indicazione delle finalità e delle modalità del trattamento e il riferimento ai soggetti ai quali i dati possono essere comunicati e all'ambito della loro diffusione.

consenso: dichiarazione di volontà con la quale l'interessato autorizza il titolare ad effettuare una o più operazioni di trattamento secondo le indicazioni fornite con l'informativa.

comunicazione: il 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;
dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
Garante: l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
Ai fini del presente Regolamento si intende, inoltre, per:
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 contraente o utente ricevente, identificato o identificabile;
chiamata: la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
reti di comunicazione elettronica: ", i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese 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 siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
rete pubblica di comunicazioni: una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti

servizio di comunicazione elettronica: ", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

"contraente": qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
dati relativi al traffico: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
dati relativi all'ubicazione: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
servizio a valore aggiunto: il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

posta elettronica: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.
Ai fini del presente Regolamento si intende, altresì, per:
misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
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) Per finalità istituzionali, ai fini del presente Regolamento, si intendono:
- le funzioni previste dalla legge, dallo Statuto, dai Regolamenti;
- le funzioni svolte per mezzo di accordi, intese, convenzioni e mediante gli strumenti di programmazione negoziata previsti dalla legislazione vigente;
- i compiti e le attività svolte in relazione ai programmi esplicitati nella Relazione Previsionale e Programmatica ed i relativi obiettivi.
3) L'Amministrazione comunale, nell'assolvimento delle proprie finalità istituzionali, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto dei diritti e delle libertà fondamentali con riferimento alla riservatezza, all'identità personale ed alla protezione dei dati delle persone fisiche e giuridiche.

Articolo 3 – Titolare del Trattamento

1. Titolare del trattamento dei dati personali effettuato dal Comune di Piana degli Albanesi, nell'ambito della propria organizzazione, è lo stesso Ente comunale nel suo complesso, rappresentato dal Sindaco che si avvale per le relative funzioni del Segretario comunale, nonché del Responsabile dei Sistemi Informativi e dei Responsabili delle direzioni.
Il Titolare provvede:
a) a richiedere, ove necessario, le autorizzazioni e ad effettuare le dovute comunicazioni al Garante per il trattamento o la comunicazione dei dati personali;
b) ad impartire ai Responsabili le necessarie istruzioni e le direttive di massima per la corretta gestione e tutela dei dati personali, ivi compresa la loro integrità e sicurezza;
c) a verificare periodicamente la corrispondenza dell'attività svolta dai Responsabili alle disposizioni di legge e regolamentari, alle istruzioni ed alle direttive impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati

Art. 4 - Responsabili del trattamento

1. I Responsabili del trattamento dei dati personali sono designati dal Titolare tra i Responsabili delle Direzioni. Essi sono responsabili di tutte le banche dati personali utilizzate dagli uffici di rispettiva competenza, nonché dei relativi trattamenti. Per esigenze organizzative il Titolare può nominare, con specifico atto, altri Responsabili, scelti tra persone che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
2. In generale, il Responsabile del trattamento, attenendosi alle istruzioni impartite dal Titolare:
a) nomina per iscritto, per quanto di competenza, gli Incaricati di ciascun trattamento, dotandoli, sulla base delle direttive di massima impartite dal Titolare, delle istruzioni per il corretto trattamento dei dati personali, specificando l'ambito del trattamento consentito a ciascuno di essi ed eseguendo gli opportuni controlli;
b) in materia di trattamento di dati sensibili e giudiziari, adotta idonee e preventive misure di sicurezza volte a dare piena attuazione alle disposizioni contenute nella vigente normativa, definendo soluzioni tecniche, informatiche, organizzative, logistiche e procedurali che tengano conto della specificità del trattamento dei dati in questione e delle particolarità connesse alle operazioni su di essi eseguibili;
c) provvede alla verifica periodica delle banche dati esistenti e stabilisce, all'occorrenza, le procedure da adottare per il trattamento di nuovi o particolari categorie di dati;
d) cura l'informativa agli interessati predisponendo, in particolare, la modulistica, o altre forme idonee di informazione nel caso di una generalità di interessati non immediatamente identificabili, inerente le attività di competenza, facendo espresso riferimento, in caso di dati sensibili e/o giudiziari, alla normativa che prevede gli obblighi o i compiti in base ai quali è effettuato il trattamento; l'informativa deve essere completa e contenere, sia pure in modo sintetico, tutte le notizie previste dall'ar. 13 del Codice;
e) vigila sulla comunicazione dei dati personali e sulla loro diffusione;
3. Il Responsabile del trattamento ha, altresì, l'obbligo:
a) di verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza e non eccedenza rispetto alle finalità istituzionali perseguite nei singoli casi disponendone, se necessario, la cancellazione totale o parziale, o il blocco qualora sia necessaria una sospensione temporanea delle operazioni di trattamento;
b) di trattare i dati sensibili e giudiziari contenuti in elenchi, registri o a banche dati, tenuti con l'ausilio di strumenti elettronici, o comunque automatizzati, mediante l'utilizzo di tecniche di cifratura, di codici
identificativi o di altri sistemi che permettono di identificare gli interessati solo in caso di necessità;
c) di conservare separatamente da ogni altro i dati idonei a rivelare lo stato di salute e la vita sessuale, adottando le cautele di cui alla lettera precedente anche quando sono tenuti in archivi o banche di dati senza l'ausilio di strumenti elettronici.

Art. 5 -Responsabile dei sistemi informativi comunali

1) Il Responsabile dei Sistemi Informativi comunali garantisce e tutela la sicurezza delle applicazioni informatiche e dei database distribuiti sulla rete nel rispetto dei principi sanciti dal Codice e collabora con il Titolare e con i Responsabili per l'individuazione delle soluzioni informatiche più idonee, tenuto conto della specificità dei trattamenti.
2) Il Responsabile della gestione e della manutenzione dei sistemi informativi comunali è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende alle risorse del sistema operativo, di un elaboratore o di un sistema di Banche di dati.

Art. 6 - Incaricati del trattamento

1. I Responsabili del trattamento dei dati provvedono, nell'ambito delle strutture di competenza, alla nomina individuale dei soggetti incaricati del trattamento.
2. L'incaricato può essere, altresì, individuato, come previsto dall'art.30, comma 2 del Codice, attraverso la documentata preposizione della persona fisica ad un'unità organizzativa per la quale è stato individuato, per iscritto, l'ambito di trattamento consentito agli addetti dell'unità medesima.
3. Gli Incaricati effettuano le operazioni di trattamento dei dati conformandosi alle istruzioni del Titolare e del Responsabile, nel rispetto della normativa vigente e della prassi interna anche per quanto riguarda gli interventi da attuare in materia di sicurezza dei dati e dei sistemi. Provvedono a fornire l'informativa agli interessati ai sensi dell'art.13 del Codice e verificano che ciascuna operazione di comunicazione e diffusione dei dati sia conforme alle disposizioni di legge e di regolamento.
4. Nei casi di trattamenti occasionali di dati che siano da svolgere da parte di soggetti non incaricati, il Responsabile del trattamento può nominare, per iscritto, tali soggetti come incaricati di specifici ambiti di trattamento e di specifiche operazioni, fornendo loro le necessarie istruzioni operative.

Articolo 7 – Individuazione delle banche dati

Le banche dati di cui all'art. 4 della del Decreto Legislativo 30 giugno 2003, n. 196, gestite dall'Ente, sono individuate su indicazione dei Responsabili del trattamento.
Le banche dati di cui al presente regolamento sono gestite in forma elettronica e cartacea.
L'Ente, di regola, provvede annualmente, alla verifica ed all'aggiornamento dell'elenco delle banche dati dei trattamenti sulla base delle relative comunicazioni inoltrate dai responsabili del trattamento.

Articolo 8 – Modalità di raccolta e requisiti dei dati personali

Il trattamento dei dati deve avvenire in modo lecito e secondo correttezza.
I dati devono possedere i requisiti dell'esattezza, della pertinenza, della completezza, dell'aggiornamento rispetto alle finalità della raccolta e del successivo trattamento, della non eccedenza rispetto alle finalità per cui sono trattati e della conservazione limitatamente agli scopi del trattamento.
Con riferimento alle modalità di raccolta i dati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi.
Le disposizioni del presente regolamento si applicano al trattamento dei dati automatizzato e, in quanto compatibili, al trattamento dei dati non automatizzato.

Articolo 9 – Trattamento dei dati personali

Il trattamento dei dati personali da parte del **Comune di Piana degli Albanesi**, svolto sia mediante l'ausilio di mezzi elettronici e comunque informatizzati, sia cartacei, è consentito esclusivamente per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla normativa vigente in materia di trattamento dei dati personali, dal presente Regolamento e dalle direttive del Garante.
Nell'ambito del trattamento dei dati sensibili e giudiziari, di cui agli artt. 20, 21 e 22 del Decreto Legislativo 30 giugno 2003, n. 196, l'Ente si attiene ai seguenti principi:
- il massimo rispetto della dignità dell'interessato, agevolando l'esercizio dei diritti di cui all'art. 7 del Decreto Legislativo 30 giugno 2003, n. 196 (accesso, correzione dati, opposizione al trattamento, ecc.);

- si possono svolgere soltanto le operazioni strettamente necessarie al perseguimento della finalità sottesa al trattamento (principio di necessità del trattamento dei dati art. 3 del Decreto Legislativo 30 giugno 2003, n. 196).
Il trattamento dei dati sensibili è consentito ai soggetti pubblici nei seguenti casi:
a) se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite;
b) nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili 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 e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo;
c) Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili.
Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2;
La comunicazione/diffusione dei dati deve avvenire nel rispetto delle disposizioni legislative e regolamentari sulla riservatezza, da combinarsi con le norme di diritto positivo in materia di accesso ai documenti amministrativi.
Nelle ipotesi in cui la legge, lo statuto o il regolamento prevedano pubblicazioni obbligatorie, il responsabile del procedimento adotta le misure eventualmente necessarie per garantire la riservatezza dei dati sensibili, di cui all'art. 20 del Decreto Legislativo 30 giugno 2003, n. 196.

I trattamenti senza l'ausilio di strumenti elettronici
Il Decreto Legislativo 196/2003 disciplina gli aspetti riguardanti:

- l'affidamento di atti o documenti contenenti dati personali agli incaricati, e la custodia da parte di questi (lettera b) del comma 1 dell'art. 35 del Codice, cui danno concreta attuazione i punti 27 e 28 del disciplinare tecnico);
- le creazione e gestione degli archivi, nei quali riporre e custodire atti e documenti contenenti dati personali quando gli stessi non sono utilizzati per lo svolgimento delle operazioni affidati agli incaricati (lettera c) del comma 1 dell'art. 35 del Codice, cui da attuazione il punto 29 del disciplinare tecnico).

Nel rispetto di quanto prescritto dal punto 27 del disciplinare tecnico agli incaricati vengono impartite istruzioni scritte su come deve avvenire il controllo e la custodia di atti e documenti contenenti dati personali di qualsiasi natura. Gli incaricati del trattamento prelevati dagli archivi i soli atti e documenti loro affidati, li devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine delle operazioni loro affidate.
Il controllo e la custodia devono avvenire in modo tale, come prescrive il punto 28 del disciplinare, in presenza di atti e documenti contenenti dati sensibili o giudiziari, che ai dati non accedano persone prive di autorizzazione. A tale fine sarà cura di ogni incaricato riporre nel cassetto della propria scrivania, che verrà chiuso a chiave, i documenti in suo possesso, prima di assentarsi, anche temporaneamente, dal posto di lavoro.
Seguendo i dettami del punto 29 del disciplinare tecnico gli atti e documenti contenenti dati sensibili e giudiziari sono conservati in archivi ad accesso controllato secondo i seguenti accorgimenti:

- gli incaricati preventivamente autorizzati ad accedere agli archivi richiedono la chiave degli stessi al custode e la restituiscono al termine dell'accesso;
- al termine dell'orario lavorativo, i nominativi di chi accede all'archivio verranno annotati in un apposito registro.

I trattamenti con strumenti elettronici

L'articolo 34 del codice e i punti da 1 a 26 del disciplinare tecnico prescrivono le misure minime di sicurezza da applicare per i trattamenti effettuati con strumenti elettronici.

Il primo ordine di prescrizioni, dettate dal primo comma dell'art. 34 del codice, impone che vengano adottati gli opportuni sistemi, al fine di consentire l'accesso agli strumenti elettronici solo a chi è autorizzato, tramite:

lettera a) l'impostazione di un sistema di autenticazione informatica, che l'articolo 4, comma 3, lettera c) del codice definisce come l'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità.

lettera b) l'adozione di procedure di gestione delle credenziali di autenticazione, che l'articolo 4, comma 3, lettera d) definisce come i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Per realizzare la credenziale di autenticazione (cioè la chiave per accedere allo strumento elettronico), l'ente ha associato un codice per l'identificazione dell'incaricato (username), attribuito dal responsabile del sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che egli stesso provvede ad elaborare, mantenere riservata e modificare periodicamente.

Il secondo ordine di prescrizioni, previste dal comma 34, disciplina l'impostazione del sistema di autorizzazione, che la lettera g) del comma 3 dell'articolo 4 definisce come 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. A tale fine, è previsto l'obbligo di:

lettera c) utilizzare un sistema di autorizzazione.

lettera d) aggiornare periodicamente l'individuazione dell'ambito del trattamento consentito ai singoli incaricati, e agli addetti alla gestione o alla manutenzione degli strumenti elettronici.

Rispettando i dettami del punto 13 e 14 del disciplinare tecnico viene limitato preventivamente l'accesso di ciascun incaricato ai soli dati necessari per effettuare le operazioni di trattamento, che si rendono indispensabili per svolgere le mansioni lavorative. Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

L'articolo 34 del codice privacy impone di:

lettera e) proteggere gli strumenti elettronici ed i dati, rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici.

lettera f) adottare procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Il punto 16 del disciplinare prevede l'obbligo di proteggere i dati personali *contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615-quinquies del codice penale*, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Si tratta dei *virus*, dai quali la norma impone di difendersi, attivando idonei strumenti elettronici, da aggiornare con cadenza almeno semestrale.

Il punto 20 aggiunge l'obbligo di adottare una ulteriore misura, in caso di trattamento di *dati sensibili o giudiziari*, imponendo di proteggerli *dall'accesso abusivo*, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici. Ai sensi dell'articolo 615-ter del codice penale, pone in essere un accesso abusivo chi *si introduce abusivamente in un sistema*

informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
La norma prevede che, nel caso in cui si trattino dati sensibili o giudiziari, non ci si possa limitare a difendersi dai programmi, ma si debbano utilizzare idonei strumenti elettronici di protezione perimetrale (ad esempio, *firewall*), per proteggersi contro l'ipotesi, ancora più pericolosa, in cui la *mente criminale* stessa tenti di accedere direttamente.
Il punto 17 prevede che, *in tutti i casi*, ci si debba dotare anche di programmi, la cui funzione è di:

- prevenire la vulnerabilità degli strumenti elettronici, non solo e non necessariamente per effetto di attacchi esterni;
- correggere i difetti insiti negli strumenti stessi.

Tra i principali punti di debolezza di un sistema informatico vanno sicuramente annoverati il sistema operativo e le applicazioni, sfruttando gli eventuali errori (*bug*) presenti nei quali degli estranei potrebbero, tra l'altro, riuscire a guadagnare l'accesso al sistema. Le contromisure da adottare sono essenzialmente di due tipi:

- l'aggiornamento costante dei prodotti, non appena viene scoperto un *bug*: tale procedura è nota come installazione di *patch*
- la verifica periodica dell'installazione e della configurazione dei prodotti software.

Sono disponibili dei programmi in grado di verificare automaticamente eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete: la norma prevede che gli ***aggiornamenti di tali programmi*** debbano essere effettuati con cadenza almeno annuale (che diviene semestrale, in caso di trattamento di dati sensibili o giudiziari), nell'ambito di un *test generale* per verificare il corretto funzionamento dell'intero sistema.
Per quanto concerne il salvataggio dei dati, al fine di consentirne il *recupero*, al verificarsi di eventi atti a distruggerli, il punto 18. prescrive che, in tutti i casi, debbano essere impartite istruzioni organizzative e tecniche, che prevedono il salvataggio dei dati *con frequenza almeno settimanale*. Per i dati *sensibili e giudiziari* il punto 23 aggiunge la prescrizione, per cui l'organizzazione deve essere in grado di provvedere, in ogni caso, al ripristino dei dati *entro sette giorni*. L'Ente ha nominato degli incaricati del backup che effettuano, periodicamente (settimanalmente), un copia di tutti i dati presenti nel sistema su dispositivi opportuni. In caso di guasto hardware dei dischi è quindi possibile ripristinare il sistema nello stesso stato in cui si trovava nel momento dell'ultimo backup.
In ottemperanza dei punti 21 e 22 del disciplinare, una particolare attenzione è stata dedicata ai supporti rimovibili contenenti dati sensibili o giudiziari, applicando le seguenti misure:

- sono custoditi ed utilizzati in modo tale da impedire accessi non autorizzati e trattamenti non consentiti: sono impartite istruzioni affinché essi vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente *formattati* quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati i supporti non vengono *abbandonati* ma vengono posti in essere gli opportuni accorgimenti, anche con la distruzione del supporto, finalizzati a rendere ***inintelligibili e non ricostruibili tecnicamente i dati*** in essi contenuti, al fine di impedire che essi vengano *carpiti* da persone non autorizzate al trattamento.

Articolo 10 – Affidamento a terzi di attività o di servizi che implichino il trattamento di dati personali.
1. Salvo diversa disciplina contenuta nelle convenzioni, nei contratti, nei disciplinari o negli altri atti che regolano in modo specifico i rapporti, il trattamento di dati personali da parte di soggetti esterni per lo svolgimento di finalità istituzionali proprie del Comune di Piana degli Albanesi è da considerare, ai fini dell'applicazione del *Codice*, come trattamento interno all'Ente.

2. In tal caso, salvo diversa specifica disciplina contenuta nei documenti regolanti il rapporto, Titolare è il Comune e Responsabile o Incaricato è il soggetto esterno che collabora con l'Ente. In specifico, nell'ambito dei trattamenti presi in considerazione nel presente articolo, il soggetto esterno qualora sia:

a) persona giuridica o pubblica amministrazione o ente o associazione, viene designato, di norma, Responsabile del trattamento dei dati personali. Esso, a sua volta, individua, all'interno della propria organizzazione, l'incaricato (o gli incaricati) per gli specifici trattamenti e dà contestuale comunicazione di tali nominativi al Comune, Titolare del trattamento;

b) persona fisica, è individuato, di regola e salvo diversa disciplina, quale Incaricato del trattamento ai sensi dell'art.7 del presente Regolamento.

3. Le convenzioni, i contratti o gli altri atti che regolano i rapporti con tali soggetti devono contenere specifiche norme che obblighino all'osservanza delle prescrizioni del *Codice*. Ai soggetti designati sono fornite, altresì, le istruzioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, per gli opportuni controlli nei limiti dell'incarico o dei rapporti contrattuali o istituzionali, individuando l'ambito di comunicazione e diffusione dei dati stessi.

4. Il Responsabile del trattamento esterno assicura al Titolare regolare ritorno di informazione sui trattamenti di competenza. Segnala, altresì, ogni fatto e situazione, rilevante ai fini del *Codice*, che richieda un suo intervento.

Articolo 11 – Diritti dell'interessato

All'interessato, i cui dati sono contenuti in una banca di dati del **Comune di Piana degli Albanesi**, spettano i diritti di cui all'art. 7 del Decreto Legislativo 196/2003 e cioè:

- di essere informato su quanto indicato in merito ai dati previsti per la notificazione;
- di ottenere, a cura del titolare o del responsabile, senza ritardo:
  - ✓ la conferma dell'esistenza o meno di trattamenti di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità del trattamento; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni;
  - ✓ la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
  - ✓ l'aggiornamento, la rettificazione, ovvero, qualora vi abbia interesse, l'integrazione dei dati;
  - ✓ l'attestazione che le operazioni di cui ai numeri 2. e 3. sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
- di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- di opporsi, in tutto o in parte, al trattamento di dati personali che lo riguardano, previsto a fini di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva e di essere informato dal titolare, non oltre il momento in cui i dati sono comunicati o diffusi, della possibilità di esercitare gratuitamente tale diritto.

L'interessato può esercitare tali diritti con una richiesta scritta al Titolare della banca di dati. La richiesta sarà ritenuta valida anche se effettuata da persone terze o associazioni munite di delega o procura scritta dell'interessato.

L'esame delle istanze per l'esercizio dei diritti compete al Responsabile del trattamento dati.
In caso di inerzia o contro il provvedimento del Responsabile del trattamento, l'interessato può proporre ricorso al Garante o all'Autorità Giudiziaria ai sensi dell'art. 56 del Decreto Legislativo 30 giugno 2003, n. 196.
Qualora , in seguito alla richiesta dell'interessato di conoscere l'esistenza di trattamenti di dati che lo riguardano, risulti l'inesistenza degli stessi, l'interessato sarà tenuto al pagamento di un contributo spese non superiore ai costi effettivamente sostenuti dall'ente.

Articolo 12 – Misure di sicurezza
I Responsabili ed il Titolare del trattamento dei dati provvedono, in relazione alla disciplina disposta del Decreto Legislativo 30 giugno 2003, n. 196, all'adozione di misure di sicurezza al fine di prevenire:
- i rischi di distruzione, perdita di dati o danneggiamento delle banche dati o dei locali ove esse sono collocate;
- l'accesso non autorizzato ai dati stessi;
- modalità di trattamento dei dati non conformi alla legge o al regolamento;
- la cessione o la distruzione dei dati in caso di cessazione di un trattamento.

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze rese disponibili dal progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Articolo 13 – Verifiche e controlli
I responsabili del trattamento provvedono, con propri atti, a dar corso alle disposizioni organizzative in materia di dati personali e sensibili, nelle articolazioni cui sono preposti.
A cura del responsabile del trattamento dei dati sono attivati periodicamente controlli, anche a campione, al fine di garantire il rispetto delle misure di sicurezza relative ai vari trattamenti e l'attendibilità dei dati trattati.
Articolo 14 – Utilizzo dei dati all'interno degli uffici dell'Ente
La comunicazione dei dati all'interno della struttura organizzativa dell'Ente, per ragioni d'ufficio e nell'ambito delle specifiche competenze, non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti. Non si considera comunicazione di dati a terzi la trasmissione e l'accesso di dati da parte del personale dipendente dell'Ente, qualora il trasferimento e l'accesso avvenga per ragioni di ufficio, nell'esercizio delle mansioni proprie di ciascun dipendente.
Il responsabile del trattamento dei dati, specie se la comunicazione concerne dati sensibili, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone, limitando l'accesso o la trasmissione dei dati sensibili ai soli casi di effettiva necessità per lo svolgimento delle funzioni ed attività dell'ente.

Articolo 15 – Comunicazione o diffusione dei dati
Una specifica attenzione va dedicata alle ipotesi di comunicazione o diffusione dei dati.
La comunicazione/diffusione dei dati è ammessa:
a) nei casi previsti dalla legge;
b) nei casi previsti dai regolamenti statali e dell'ente;
c) in altri casi in cui la comunicazione di dati a soggetti pubblici sia necessaria per lo svolgimento delle loro funzioni istituzionali, previa autorizzazione del Garante. Non è mai possibile comunicare dati ai privati fuori dai casi previsti sub "a" e "b".