INDICE

INTRODUZIONE

Gli articoli 31 e seguenti del Decreto Legislativo 30 giugno 2003 n. 196, denominato "Codice in materia di protezione dei dati personali" e l'Allegato B del Codice, denominato "Disciplinare tecnico in materia di misure minime di sicurezza", prescrivono l'obbligo per il Comune di **Terragnolo** di implementare le misure di sicurezza idonee e preventive in modo da ridurre al minimo i rischi connessi al trattamento dei dati personali.

La policy di sicurezza del trattamento dei dati personali assume una rilevanza strategica per l'ente, considerata in particolare la qualità e quantità dei dati personali trattati e altresì la responsabilità che deriva dal loro trattamento.
Il decreto legge 9 febbraio 2012 n. 5, in vigore dal 10 febbraio 2012, convertito in legge 4 aprile 2012 n 35, all'art. 45, ha modificato il decreto legislativo 30 giugno 2003 n. 196 (Codice privacy), abolendo l'obbligo di redazione e aggiornamento del Documento programmatico sulla sicurezza.

Resta obbligatoria l'adozione di tutti gli altri adempimenti giuridico-amministrativi e delle misure di sicurezza.
Venuta meno l'obbligatorietà di adottare e aggiornare annualmente il DPS, il Comune di **Terragnolo** al fine di dare continuità al proprio programma di gestione sicura dei dati personali a garanzia del primario diritto dei cittadini alla riservatezza e alla dignità personale, afferma a fortiori **l'opportunità e l'utilità** di adottare e aggiornare un **documento programmatico in materia privacy (DPP).**
Il Comune di **Terragnolo** ha quindi predisposto ed adottato per l'anno 2015 il presente DPP.
Venuto meno l'obbligo normativo, lo spirito con il quale lo stesso è stato predisposto è la consapevolezza che questa, assieme ad altre misure, contribuisce a garantire un sicuro e legittimo trattamento dei dati personali dei propri cittadini.
Il DPP è un documento che rappresenta la struttura organizzativa del Comune di **Terragnolo**, evidenziandone le dotazioni di risorse umane, fisiche e tecnologiche e che fornisce una fotografia reale della policy che l'ente ha adottato ed intende adottare per garantire la protezione, l'integrità e la sicurezza dei dati personali trattati.

OBIETTIVI DEL DOCUMENTO

- individuare, analizzare e valutare i rischi al patrimonio informativo del Comune di **Terragnolo** e determinare le misure di sicurezza idonee a garantire la protezione dei dati personali;
- ottemperare agli adempimenti previsti dal Codice in materia di protezione dei dati personali.

METODOLOGIA

Nella redazione del DPP è stata utilizzata una metodologia che soddisfa rigorosamente il dettato normativo contenuto nel Disciplinare tecnico in materia di misure minime di sicurezza.

La realizzazione del DPP segue un processo di analisi con cadenza annuale così essenzialmente strutturato:

- analisi qualitativa del patrimonio informativo;
- individuazione dei ruoli e delle responsabilità;
- identificazione dei luoghi fisici ove sono custoditi e trattati le informazioni e i dati personali;
- identificazione delle risorse hardware con cui vengono custoditi e trattati le informazioni e i dati personali;
- identificazione delle risorse software con cui vengono custoditi e trattati le informazioni e i dati personali;
- identificazione e classificazione delle informazioni e dei dati personali trattati;
- analisi dei rischi;
- individuazione dei criteri tecnici e organizzativi per la protezione delle aree e dei locali;
- individuazione delle procedure per il controllo degli accessi ai locali;
- individuazione dei criteri e delle procedure per assicurare l'integrità dei dati, per la sicurezza delle trasmissioni anche per via telematica;
- individuazione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a danneggiamento o distruzione;
- individuazione dei criteri da adottare per garantire l'adozione delle misure di sicurezza in caso di trattamenti affidati all'esterno;
- elaborazione di un piano di verifica.

Operativamente il documento consta di due sezioni.

FINALITÀ DELLA LEGGE E DEFINIZIONI

OGGETTO DELLA DISCIPLINA DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003 n. 196) disciplina il trattamento dei dati personali, al fine di garantire che lo stesso si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (art. 2, comma 1).

Il diritto alla protezione del dato personale trova fondamento in diritti delle persona "sovraordinati", riconosciuti come inviolabili e fondamentali dall'articolo 2 della Costituzione, quali:

- **il diritto alla riservatezza**, quale il diritto a mantenere libera da ingerenze esterne la propria vita privata;
- **il diritto all'identità personale**, quale diritto ad utilizzare in esclusiva il proprio nome e altri elementi identificativi della persona;
- **il diritto all'autodeterminazione informativa**, quale nuovo e fondamentale diritto al controllo e alla "gestione" dei propri dati personali.

DEFINIZIONE DI DATI PERSONALI

Dato personale è qualunque informazione idonea a identificare una persona fisica in modo diretto o indiretto, vale a dire anche quando l'identificazione sia possibile attraverso il collegamento di più informazioni di per sé non significative, se singolarmente considerate.

Il Codice definisce come **dati identificativi** i dati che consentono di identificare in maniera diretta una persona.

Il Codice individua, tra i dati personali, alcune particolari categorie: dati sensibili, dati giudiziari, altri dati particolari, dati comuni.

DEFINIZIONE DI DATI SENSIBILI

Sono i dati personali individuati dall'art. 4, comma 1, lettera d, del Codice, 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 o organizzazioni a carattere religioso, filosofico, politico o sindacale; lo stato di salute e la vita sessuale.

La definizione di dato sensibile è **esclusiva**. Sono considerati tali solo i dati specificamente indicati, indipendentemente dal carattere di riservatezza o di particolare rilevanza che un individuo o il senso comune può attribuire ad altre tipologie di dati (ad esempio: codice identificativo della carta di credito, reddito, stato di separazione, ecc.).

DEFINIZIONE DI DATI GIUDIZIARI

Sono i dati personali indicati dall'articolo 4, comma 1, lettera e del Codice, idonei a rivelare i provvedimenti di cui all'articolo 686, commi 1, lettere a) e d), 2 e 3, del Codice di procedura penale.

Riguardano le iscrizioni al casellario giudiziario in materia penale, quali ad esempio: condanna penale, dichiarazione di abitualità nel reato, pene accessorie ecc.

DEFINIZIONE DEGLI ALTRI DATI PARTICOLARI

Si tratta di un'ulteriore categoria prevista dall'articolo 17 del Codice, il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. Il loro trattamento è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato ove prescritti dal Garante.

DEFINIZIONE DI BANCA DATI

È qualsiasi insieme di dati personali organizzati in modo da renderne possibile o agevole la consultazione e il trattamento.

Non si considerano, pertanto, le sole "raccolte" informatizzate, bensì tutte le raccolte di dati personali, a prescindere dallo strumento usato per il trattamento dei dati, comprendendo anche strumenti di archiviazione quali i supporti audiovisivi, ottici, fotografici e le "raccolte" cartacee. Ai fini dell'applicazione delle misure di sicurezza, sono rilevanti non solo le banche dati ufficiali, ma anche le semplici raccolte di dati personali finalizzate all'ordinaria gestione dell'attività amministrativa.

DEFINIZIONE DI TRATTAMENTO DI DATI PERSONALI

Costituisce trattamento di dati personali (art. 4 lettera a del Codice) qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, 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.

DEFINIZIONI DI COMUNICAZIONE E DI DIFFUSIONE

La **comunicazione** è l'operazione di trattamento che consiste nel portare i dati personali a **conoscenza di uno o più soggetti determinati** (identificabili in modo univoco e determinato), diversi dall'interessato, cui i dati stessi si riferiscono, in qualunque forma, anche mediante la loro messa a disposizione per la consultazione.

Non è comunicazione la conoscenza di dati di incaricati delle strutture interne del Comune o di soggetti esterni individuati come responsabili o incaricati del trattamento nell'ambito di attività di *outsourcing* o in base ad atto convenzionale (ad es.: affidamento all'esterno di compiti del Comune). In tal caso anche i soggetti esterni che collaborano con il Comune sono considerati parte della "struttura organizzativa privacy" della stessa.

La **diffusione** è l'operazione di trattamento che consiste nel portare i dati personali a **conoscenza di un numero di soggetti indeterminati**, in qualunque forma, anche mediante la loro messa a disposizione per la consultazione.

Tipica forma di diffusione è quella che si realizza tramite registri o albi pubblici ovvero con la pubblicazione dei provvedimenti all'albo pretorio telematico o sulla rete civica.

PRESUPPOSTI CHE LEGITTIMANO IL TRATTAMENTO DEI DATI PERSONALI DA PARTE DEI SOGGETTI PUBBLICI

Ai sensi dell'art. 18 del Codice, il trattamento di dati personali da parte dei soggetti pubblici, esclusi gli enti pubblici economici, è consentito soltanto:

- per lo svolgimento delle funzioni istituzionali;

- nei limiti dettati da leggi e regolamenti.

I soggetti pubblici devono applicare quanto previsto dall'articolo 3 del Codice (principio di necessità). I sistemi informativi e i programmi informatici vanno configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

In presenza dei suddetti presupposti giuridici, i soggetti pubblici possono legittimamente trattare i dati personali, **senza acquisire il consenso** dell'interessato.

Al contrario, l'acquisizione del consenso dell'interessato **non legittima** i soggetti pubblici a trattare dati per finalità diverse da quelle istituzionali o a effettuare operazioni non consentite da leggi o regolamenti.

PRESUPPOSTI CHE LEGITTIMANO LA COMUNICAZIONE E LA DIFFUSIONE DEI DATI PERSONALI DA PARTE DEI SOGGETTI PUBBLICI

La disciplina si differenzia a seconda del soggetto destinatario.

Comunicazione o diffusione a soggetti pubblici:

la comunicazione e la diffusione a soggetti pubblici, esclusi gli enti pubblici economici, dei dati trattati **sono ammesse** (art. 19 del Codice) quando siano previste da norme di legge o di regolamento o quando risultino comunque necessarie per lo svolgimento delle funzioni istituzionali; in questo caso, mancando una disposizione normativa o regolamentare, va data previa comunicazione al Garante.

Comunicazione o diffusione a privati o enti pubblici economici:

la comunicazione e la diffusione dei dati personali da parte di soggetti pubblici a privati o a enti pubblici economici sono ammesse solo quando siano previste da norme di legge o di regolamento (art. 19, comma 3, del Codice).

DIFFUSIONE DEI DATI RELATIVI ALLO STATO DI SALUTE

Esiste un **generale divieto di diffusione dei dati relativi allo stato di salute**.

MISURE DI SICUREZZA

Le **misure di sicurezza** sono costituite dal complesso delle misure organizzative, tecniche, informatiche, logistiche e procedurali finalizzate a ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei dati;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta;
- modifica dei dati in conseguenza di interventi non autorizzati o non conformi alla regole.

Tutti i titolari sono tenuti ad adottare le misure minime di sicurezza individuate dagli artt. 31 e seguenti del Codice e secondo le modalità previste nel Disciplinare tecnico allegato B) al Codice.

La mancata sicura custodia dei dati è causa di un danno.

Il soggetto che non adotta le misure minime di sicurezza previste dalla legge e di propria competenza è responsabile penalmente e amministrativamente (se le misure non rispettano le prescrizioni indicate nel Disciplinare Tecnico) e civilmente per il risarcimento del danno (se le misure non sono idonee).

Ai sensi dell'art. 31 del Codice le misure di sicurezza adottate per il trattamento dei dati personali devono essere:

- adeguate in relazione alle conoscenze acquisite in base al progresso tecnico e tali da ridurre al minimo i rischi di distruzione dei dati o accesso non autorizzato;
- adottate in via preventiva e differenziate in base alla natura dei dati e alle specifiche caratteristiche del trattamento.

Mancata adozione di:	**Conseguenze:**		
	Resp. Amm.	Resp. Penale	Resp.Civile
misure di sicurezza minime	Si	Sì	Sì
misure di sicurezza idonee	No	No	Sì

Le conseguenze della mancata adozione di misure di sicurezza sono quindi le seguenti

- la **sanzione penale e amministrativa** per omessa adozione delle misure minime previste dagli artt. 162 e 169 del Codice;
- **il risarcimento del danno** nel caso le misure adottate non siano idonee ad evitare il danno, ai sensi dell'art. 15 legge del Codice. Il dettato normativo fa rinvio all'art. 2050 del Codice Civile, stabilendo quindi una presunzione di colpa a carico del responsabile del danno (chi effettua il trattamento). Spetta allo stesso l'onere della prova di aver adottato tutte le misure idonee ad per evitare il danno.

La mancata applicazione delle misure di sicurezza predisposte e implementate dal titolare del trattamento e l'inosservanza delle ulteriori indicazioni impartite dallo stesso o dal responsabile da luogo a possibile **responsabilità disciplinare, civile e penale a carico degli incaricati**.

DISPOSIZIONI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

Ogni trattamento di dati personali è consentito al Comune, in quanto soggetto pubblico, qualora sussistano i presupposti previsti dall'articolo 18 del Codice. Esso deve svolgersi nel rispetto delle regole prescritte dall'art. 11 del Codice. In particolare:

- va privilegiato, ove possibile, il trattamento di dati anonimi;
- se non è possibile il perseguimento delle finalità istituzionali mediante il trattamento di dati anonimi, va comunque garantita l'osservanza dei principi di necessità, pertinenza e non eccedenza rispetto alle finalità del trattamento, ai sensi degli artt. 3 e 11 del Codice.

I dati personali devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi ed in funzione dello svolgimento di compiti istituzionali, nei limiti stabiliti dalle leggi e dai regolamenti;
- esatti e, se necessario, aggiornati;
- trattati da soggetti incaricati del trattamento, nominati dal titolare o dal responsabile del trattamento o eventualmente trattati dallo stesso responsabile;
- trattati per il tempo strettamente necessario per lo svolgimento dei compiti istituzionali; i documenti e gli altri supporti nei quali sono contenuti i dati personali devono essere conservati con modalità da garantirne l'integrità e la sicurezza.

Ai fini della sicurezza dei dati personali:

- le riproduzioni di documenti equivalgono ai documenti stessi e, pertanto, vanno gestiti con le medesime cautele;
- qualunque prodotto dell'elaborazione di dati personali, ancorché non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, elaborazioni temporanee ecc.), va trattato con le stesse cautele che sarebbero riservate alla versione definitiva.

DISPOSIZIONI SPECIALI PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI

Il trattamento dei dati personali sensibili e giudiziari è soggetto ad una disciplina speciale, individuata, in particolare, dagli articoli 20, 21 e 22 del Codice.

Il trattamento dei dati sensibili e giudiziari:

- è consentito solo se autorizzato da un'espressa **disposizione di legge**, nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite;
- in mancanza di un'espressa disposizione di legge, i soggetti pubblici **possono richiedere al Garante per la protezione dei dati personali** l'individuazione delle attività che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato 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 con atto di natura regolamentare adottato in conformità al parere espresso dal Garante;
- nei casi in cui sia specificata dalla legge o da un provvedimento del Garante per la protezione dei dati

personali la finalità di rilevante interesse pubblico, ma non sono specificati i tipi di dati e le 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 del Codice, con **atto di natura regolamentare** adottato in conformità al parere espresso dal Garante.

L'articolo 22 del Codice individua i principi applicabili al trattamento dei dati sensibili e giudiziari:

- i soggetti pubblici sono autorizzati a trattare esclusivamente i dati sensibili e giudiziari essenziali per lo svolgimento delle attività istituzionali che non possono essere adempiute mediante il trattamento di dati anonimi o di dati personali non sensibili. Si possono svolgere le sole operazioni di trattamento strettamente necessarie per il perseguimento delle finalità per le quali il trattamento è consentito (principi di pertinenza e non eccedenza);
- nell'**informativa** di cui all'art. 13 del Codice, l'interessato, cui i dati sensibili e giudiziari si riferiscono va informato circa le disposizioni legislative che prevedono gli obblighi o i compiti per i quali deve essere eseguito il trattamento e le finalità per cui i dati sono raccolti;
- i dati sensibili e giudiziari possono essere **comunicati o diffusi** nei limiti di quanto previsto da disposizioni di **legge** o dai provvedimenti assunti ai sensi dell'articolo 20;
- i dati relativi alla salute **non possono essere oggetto di diffusione** (comma 8, art. 22);
- vi è l'obbligo di **custodia separata** dei dati relativi allo stato di salute ed alla vita sessuale rispetto agli altri dati trattati per finalità che non richiedono il loro utilizzo;
- sono previste misure di sicurezza particolari.

PARTE I

BREVE DESCRIZIONE DELLA RETE INFORMATICA

Contenuti

Nella sezione è descritta la struttura informatica dell'Ente.

Numero di server presenti	2
Tipo di piattaforma dei server (Microsoft – Linux – Unix…)	Microsoft
Numero di computer	7 + 2 notebook
Tipo di piattaforma dei client (Microsoft – Linux – Mac)	Microsoft
Utilizzo di computer portatili	SI
Sistema con un unico dominio	SI
Presenza di UPS	SI
Presenza di VPN o connessioni verso altre reti esterne o computer remoti	NO
Tipologia di collegamenti (cavo di rete – wireless)	Cavo di rete
Tipologia di connessione a internet	Hyper LAN Trentino Network A breve FIBRA
Presenza di un firewall	SI
Presenza di sistema antivirus	SI
Tipologia di backup	Macrium + Synckback
Aggiornamento del sistema operativo	SI
Verifica dei backup (controllo dei log) e prove di restore	Controllo dei log e restore già fatto in caso di necessità
Gestione password utente administrator	GREAD

PARTE II

ELENCO DEI TRATTAMENTI DI DATI PERSONALI – RESPONSABILI, INCARICATI E AMMINISTRATORI DI SISTEMA – BANCHE DATI E STRUMENTI (REGOLA 19.1 – REGOLA 19.2)

Contenuti

In questa sezione sono individuati i trattamenti effettuati dal titolare, con l'indicazione della natura dei dati e della struttura organizzativa che li tratta.

Sono altresì indicate le banche dati e gli strumenti utilizzati per il trattamento dei dati.

INFORMAZIONI ESSENZIALI

Tabella 1

Descrizione Sintetica: è menzionato il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es. fornitura di beni e servizi, gestione del personale ecc.).

Natura dei dati trattati: è indicato se sono trattati dati personali o anche dati sensibili o giudiziari.

Struttura di riferimento: è indicata la struttura (ufficio, servizio, ecc.) che effettua il trattamento. In caso di strutture complesse, è possibile indicare la macro-struttura (direzione, dipartimento o servizio del personale), oppure gli uffici specifici all'interno della stessa.

Responsabili: sono individuati i responsabili del trattamento.

Incaricati: sono individuati gli incaricati del trattamento.

Tabella 1 – Elenco dei trattamenti: informazioni essenziali – responsabili e incaricati

Descrizione sintetica	Natura dei dati trattati (A, P, S, G)	Struttura di riferimento	Responsabili e Incaricati
Gestione organi istituzionali Gestione relazioni istituzionali Gestione contrattualistica Gestione appalti Gestione comunicazione istituzionale Gestione contenzioso Gestione formazione del personale Gestione attività culturali, sportive e del tempo libero Gestione statistica Gestione protocollo e notificazioni Gestione archivi Gestione rapporti con i cittadini e utenti	P – S - G	Segreteria	Vedi atti di nomina
Gestione giuridica ed economica del personale Gestione concorsi pubblici Gestione rapporti con i cittadini e utenti Gestione relazioni con altri soggetti pubblici	P – S – G	Segreteria	Vedi atti di nomina

Gestione entrate Gestione bilancio Gestione contabilità Gestione finanziaria Gestione economato Gestione dei fornitori Gestione inventario Gestione rapporti con i cittadini e utenti Gestione relazioni con altri soggetti pubblici	P – S	Ragioneria	Vedi atti di nomina
Gestione accertamento e riscossione tasse, imposte e tariffe Gestione rapporti con i cittadini e utenti Gestione relazioni con altri soggetti pubblici	P - S	Tributi	Vedi atti di nomina
Gestione anagrafe Gestione stato civile Gestione elettorale Gestione rapporti con i cittadini e utenti Gestione relazioni con altri soggetti pubblici	P – S – G	Anagrafe	Vedi atti di nomina
Gestione commercio Gestione rapporti con i cittadini e utenti Gestione relazioni con altri soggetti pubblici	P – S – G	Anagrafe	Vedi atti di nomina
Gestione edilizia privata Gestione urbanistica Gestione viabilità e reti Gestione traffico e trasporti Gestione ambiente Gestione rapporti con i cittadini e utenti Gestione relazioni con altri soggetti pubblici	P – S - G	Tecnico	Vedi atti di nomina
Gestione edilizia pubblica Gestione lavori pubblici Gestione del patrimonio Gestione protezione civile Gestione rapporti con i cittadini e utenti Gestione relazioni con altri soggetti pubblici	P – S - G	Tecnico	Vedi atti di nomina

Gestione competenze polizia locale e servizi di polizia stradale Gestione polizia annonaria Gestione controllo dell'attività edilizia Gestione controllo commercio Gestione tutela ambientale Gestione protezione civile Gestione attività di polizia giudiziaria Gestione pubblica sicurezza Gestione rapporti con i cittadini e utenti Gestione relazioni con altri soggetti pubblici	P – S - G	Polizia Municipale	Vedi atti di nomina

A = dati anonimi

P = dati personali

S = dati sensibili

G = dati giudiziari

Tabella 2

Tabella 2 – Amministratori di Sistema

Sono indicati gli Amministratori di sistema dell'Ente e il tipo di incarico agli stessi affidato.

n°	Nome e Cognome/ Ragione sociale	Funzioni e compiti affidati
1	Vedi atti di nomina	Gestione e manutenzione del sistema informatico
2	Vedi atti di nomina	Gestione e manutenzione software in dotazione

Tabella 3

Banca dati: è indicata la banca dati (ovvero il data base o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i dati.

Luogo di custodia dei supporti di memorizzazione: è indicato il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano (in quale sede, centrale o periferica, ecc.), gli elaboratori su cui sono memorizzati i dati, i luoghi di conservazione dei supporti utilizzati per le copie di sicurezza (nastri, CD, ecc) ed ogni altro supporto rimovibile.

Tipologia di dispositivi: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale, palmare, telefonino, ecc.

Tipologia di interconnessione: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, internet, ecc.

Tabella 3 – Banche dati e strumenti

Banca dati	Luogo di Custodia	Tipologia di dispositivi di accesso	Tipologia di interconnessione
Server	Sede	PC	LAN

Archivi cartacei

Descrizione	Tipo di dati	Struttura	Custodia
Archivio personale	P – S- -G	Segreteria	Serratura con chiave
Archivio contabile	P – S- -G	Ragioneria	Serratura con chiave
Archivio tributi	P – S- -G	Tributi	Serratura con chiave
Archivio anagrafe e elettorale	P – S- -G	Anagrafe	Serratura con chiave
Archivio fornitori	P – S- -G	Ragioneria	Serratura con chiave
Archivio appalti e contratti	P – S- -G	Segreteria	Serratura con chiave
Archivio tecnico	P – S- -G	Tecnico	Serratura con chiave

ANALISI DEI RISCHI PER IL TRATTAMENTO DEI DATI PERSONALI (REGOLA 19.3)

Contenuti

In questa sezione sono descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati e vengono valutate le possibile conseguenze e le gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti utilizzati.

INFORMAZIONI ESSENZIALI

Tabella 1

Elenco degli eventi: sono individuati ed elencati gli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali. In particolare, è presa in considerazione la lista esemplificativa dei seguenti eventi:

- **comportamenti degli operatori:**
  - sottrazione di credenziali di autenticazione;
  - carenza di consapevolezza, disattenzione e incuria;
  - comportamenti sleali e fraudolenti;
  - errore materiale.
- **eventi relativi agli strumenti:**
  - azione di virus informatici o di programmi suscettibili di recare danno;
  - spamming o tecniche di sabotaggio;
  - malfunzionamento, indisponibilità o degrado degli strumenti;
  - accessi esterni non autorizzati;
  - intercettazione di informazioni in rete.
- **eventi relativi agli strumenti**
  - ingressi non autorizzati a locali/aree ad accesso ristretto;
  - sottrazione di strumenti contenenti dati;
  - eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.);
  - guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.);
  - errori umani nella gestione della sicurezza fisica.

Impatto di sicurezza: sono descritte le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento e sono valutate la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'evento (anche in termini sintetici: es, alta/media/bassa).

Tabella 1 – Analisi dei rischi

Evento		Impatto sulla sicurezza dei dati				
		Id Rischio	Descrizione Rischio	Gravità Evento	Probabilità Evento (attuale)	Indice Qualitativo Gravità
Comportamenti degli operatori	furto di credenziali di autenticazione	1	Il furto delle credenziali permetterebbe di avere accesso a dati di cui non si è autorizzati al trattamento	8	2	1,6
	carenza di consapevolezza, disattenzione o incuria	2	La condivisione della conoscenza della propria password con altri utenti permette a questi e a chiunque conosca quest'informazione di accedere a dati sensibili di cui non si è autorizzati al trattamento	8	3	2,4
	comportamenti sleali o fraudolenti	3	Il trattamento effettuato per fini diversi da quelli strettamente necessari all'espletamento del proprio lavoro può provocare furto, cancellazione e modifica dei dati	7	3	2,1
	errore materiale	4	Un errore umano durante il trattamento può provocare danni come la cancellazione, la modifica e la scrittura errata di dati	6	4	2,4
Eventi relativi agli strumenti	azione di virus informatici o di codici malefici	5	L'azione di Virus o codice malefico può provocare la perdita dei dati, così come il blocco del sistema con la conseguente inaccessibilità ai dati stessi	10	3	3,0
	spamming o altre tecniche di sabotaggio	6	L'uso di tecniche di sabotaggio ed attacchi di tipo Denial of Service possono provocare un blocco al sistema	9	3	2,7
	malfunzionamento, indisponibilità o degrado degli strumenti	7	Il blocco del Server può provocare il blocco dell'accesso ai dati e la conseguente impossibilità di effettuare i trattamenti degli stessi	10	3,8	3,8
	accessi esterni non autorizzati	8	Un accesso esterno non autorizzato può permettere la copia, la cancellazione, la modifica e la scrittura errata dei dati	10	3	3,0
	intercettazione di informazioni in rete	9	L'intercettazione delle informazioni in rete può consentire l'accesso a dati di cui non si è autorizzati al trattamento	8	3	2,4
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	10	L'accesso non autorizzato al locale dove è situato il server può comportare danni al sistema, furto dei dati e delle attrezzature	8	3	2,4
	asportazione e furto di strumenti contenenti dati	11	I supporti di memorizzazione contenenti dati sensibili possono essere rubati e permettere un accesso non autorizzato ad informazioni sensibili e/o giudiziarie	8	4	3,2
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	12	La distruzione dell'apparecchiatura o dell'intero locale ove è situato il server può provocare la perdita dei dati nonché l'impossibilità fisica di riprendere il servizio	10	3,8	3,8
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	13	Il guasto a sistemi complementari può comportare la corruzione dei dati così come il blocco del servizio di trattamento erogato	8	4	3,2
	errori umani nella gestione della sicurezza fisica	14	L'errore umano nella gestione delle regole di sicurezza fisica impartite può comportare guasti e/o la compromissione delle contromisure adottate	8	4	3,2

N.B. L'indice qualitativo di gravità è dato dalla seguente formula = (Gravità evento * Probabilità attuale evento)/10

Gravità evento: rappresenta il valore assegnato su scala decimale (1 minimo - 10 massimo) rispetto alla pericolosità che l'evento può assumere in relazione alla sicurezza dei dati.

Probabilità evento (attuale): rappresenta il valore assegnato su scala decimale (1 minimo - 10 massimo) rispetto alla possibilità che l'evento possa verificarsi in relazione alle misure attualmente implementate.

Indice qualitativo di gravità: rappresenta il valore su scala decimale (1 minimo - 10 massimo) espressione del rapporto tra gravità dell'evento e la probabilità che lo stesso si verifichi secondo la formula **Indice qualitativo = Gravità evento * Probabilità evento / 10.**

Se l'indice qualitativo di gravità è uguale o maggiore al valore di 4, pur avendo adottato le misure minime di sicurezza, si evidenzia la necessità di attivare nuove misure che abbiano l'effetto di ridurre ulteriormente il rischio.

Tabella 2 Misure di Sicurezza implementate o da implementare

MISURE DI SICUREZZA IN ESSERE E DA ADOTTARE (REGOLA 19.4)

Contenuti

In questa sezione sono riportate in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati.

Per misura di sicurezza si intende lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti derivanti da una specifica minaccia.

Nella tabella 1 sono indicate le macro-misure di sicurezza implementate per eliminare o ridurre i rischio individuati.

Nella tabella 2 sono specificate, nell'ambito di ogni macro-misura di sicurezza, quali misure di sicurezza sono già implementate e quali sono da implementare.

Tabella 1 - Rischio – Macro-misure di sicurezza

Rischio	Macro Misura Sicurezza
furto di credenziali di autenticazione	Sistema di Autenticazione
	Formazione
carenza di consapevolezza, disattenzione o incuria	Sistema di Autenticazione
	Formazione
comportamenti sleali o fraudolenti	Sistema di Autorizzazione
errore materiale	Protezione dalla perdita dei dati
	Formazione
azione di virus informatici o di codici malefici	Sistema di protezione da codice malizioso
spamming o altre tecniche di sabotaggio	Sistema di Sicurezza per accessi non autorizzati
	Sistema di Sicurezza per la protezione della Posta
malfunzionamento, indisponibilità o degrado degli strumenti	Sistema di Sicurezza per accessi non autorizzati
accessi esterni non autorizzati	Sistema di Sicurezza per accessi non autorizzati
intercettazione di informazioni in rete	Sistema di Sicurezza per accessi non autorizzati
accessi non autorizzati a locali/reparti ad accesso ristretto	Sistema di Sicurezza Fisica
asportazione e furto di strumenti contenenti dati	Sistema di Sicurezza Fisica
eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Piano di Alta Affidabilità e di Disaster Recovery
	Formazione
guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	Piano di Alta Affidabilità e di Disaster Recovery
errori umani nella gestione della sicurezza fisica	Formazione

Descrizione Misura di sicurezza	Riferimento Macro Misura di sicurezza	Chi implementa la misura?	Misure minime		Misure idonee[1]
			In essere	Da adottare	In essere
Associazione individuale di una o più credenziali per l'autenticazione dei files	Sistema di autenticazione	I	X		
Associazione individuale di una o più credenziali per l'autenticazione degli applicativi		A	X		
Disattivazione delle credenziali se non utilizzate da almeno sei mesi o in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali		A	X		
Password composte da almeno otto caratteri		A –I	X		
Password non contenenti riferimenti agevolmente riconducibili all'incaricato		I	X		
Soluzione tecnica per la modifica delle password, impostate dall'amministratore di sistema, da parte dell'utente al primo utilizzo		A	X		
Soluzione tecnica per la modifica obbligatoria delle password almeno ogni tre mesi		A	X		
Istruzioni agli incaricati delle regole per la corretta gestione delle credenziali di autenticazione e/o delle password		T- R	X		

[1] Si tratta di misure di sicurezza ulteriori rispetto a quelle minime, opportune ed idonee per garantire una migliore sicurezza dei dati personali

Individuazione e assegnazione dei diversi ruoli dei trattamenti (titolare, responsabili, incaricati, amministratori di sistema) e loro nomina	Sistema di Autorizzazione	T- R	X		
Definizione e assegnazione dei profili di autorizzazione		T- R	X		
Verifica semestrale dei profili di autorizzazione		A	X		
Definizione di regole, compiti e responsabilità per il back-up dei dati	Protezione della perdita dei dati	R – A	X		
Pianificazione di prove di ripristino dei dati		A	X		
Istruzioni agli incaricati relative alle regole da seguire per il back-up dei dati		R -A	X		
Istruzioni agli incaricati relative alle regole da osservare per il ripristino dei dati		R	X		
Definizione di regole puntuali per il back-up dei dati		A – R	X		
Verifica periodica del funzionamento del sistema di ripristino dei dati		A	X		
Definizione e implementazione di un sistema di antivirus client / server	Sistema di protezione da codice malizioso	A	X		
Definizione e implementazione di un sistema di antivirus per server		A	X		
Definizione e implementazione di un sistema di antivirus per i client		A	X		X

Utilizzo di software anti-spyware		A	X		
Utilizzo di un sistema firewall hardware di proprietà	Sistema di sicurezza per accessi non autorizzati	A	X		
Utilizzo di un sistema firewall tramite rete Telpat gestita da Informatica Trentina spa		A	X		
Sistema idoneo alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema		A	X		
Sistemi di crittografia	Sistema di sicurezza per la protezione della posta elettronica	A		X	
Sistemi con firma digitale		A		X	
Sistema di gestione della posta elettronica		A	X		
Istruzioni agli incaricati per il corretto utilizzo del sistema di gestione della posta elettronica		T - R	X		

Definizione e realizzazione di un piano di continuità operativa e di Disaster Recovery	Piano di continuità operativa e di Disaster Recovery	A		X	
Contratti di assistenza per sostituzione e ripristino attività server		A-R	X		
Aggiornamento dei sistemi operativi (Patch)		A	X		
Installazione di sistemi UPS (gruppo statico di continuità) per i server		A	X		
Installazione di sistemi UPS (gruppo statico di continuità) per i client		A	X		
Installazioni di sistemi di raffreddamento per il locale del Server		A	X		
Realizzazione di verifiche periodiche del piano di Disaster Recovery		A		X	
Definizione di un piano di misure di sicurezza fisica	Sistema di sicurezza fisica	R	X		
Implementazione misura di controllo degli accessi fisici (allarmi, altro)		T	X		
Implementazione misure di sicurezza degli archivi (armadi a chiave, serrature delle porte di accesso, custodia chiavi)		R	X		
Implementazione misure per rischi da allagamento o incendio		T-R	X		
Istruzioni agli incaricati per la gestione della sicurezza fisica		R	X		
Sistema di videosorveglianza		R	X		
Sistema di controllo degli accessi di persone non incaricate dopo l'orario di chiusura degli uffici		R	X		
Sistema di controllo degli accessi di persone non incaricate		R	X		
Formazione ad incaricati e responsabili sul ruolo e i compiti	Formazione	R	X		
Formazione agli incaricati specifica sulle misure informatiche		R	X		
Formazione periodica agli incaricati sulla gestione della sicurezza Fisica		R	X		

A = amministratore di sistema

T = titolare

R= responsabile

I = incaricato

CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI (REGOLA 19.5)

In questa sezione sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di perdita dei dati.

L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo. E' essenziale che, quando necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci.

Sono descritti sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino.

Tabella 1 – Criteri e procedure per il salvataggio dei dati

Backup Exec per copia dati e componenti di sistema (su cassetta LTO Tandberg)
Syncback Pro per copia con versioning del Fileserver (su NAS di rete giornaliero)
Macrium Reflect per copia immagine sistema operativo (su NAS di rete giornaliero)

Tabella 2 – Criteri e procedure per il ripristino della disponibilità dei dati

Danneggiamento sistema operativo (ripristino da LTO Tandberg o da immagine sistema operativo da software Macrium)
Perdita di file cancellati erroneamente, recupero da NAS tramite Syncback pro (disponibili più versioni dello stesso file) oppure da cassetta TANDBERG

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI (REGOLA 19.6)

In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

Informazioni essenziali

Descrizione sintetica degli interventi formativi: sono descritti sinteticamente gli obiettivi e le modalità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 (ingresso in servizio o cambiamento di mansioni degli incaricati, introduzione di nuovi elaboratori, programmi o sistemi informatici, ecc.).

Tempi previsti: sono indicati i tempi previsti per lo svolgimento degli interventi formativi.

Tabella 1 – Pianificazione degli interventi formativi previsti

Descrizione sintetica degli interventi formativi	Tempi previsti
Il corso avrà ad oggetto l'illustrazione sintetica del quadro normativo e delle novità legislative nonché dei recenti provvedimenti del Garante, con specifica e particolare attenzione alle implicazioni organizzative - comportamentali della normativa rispetto all'attività di servizio	31.12.2015

Tabella 2 – Interventi formativi già attivati

Descrizione sintetica degli interventi formativi	Data Intervento

TRATTAMENTI AFFIDATI ALL'ESTERNO (REGOLA 19.7)

Contenuti

E' redatto un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati di cui è titolare l'ente.

Informazioni essenziali

Descrizione dell'attività "esternalizzata": è indicata sinteticamente l'attività affidata all'esterno.

Trattamenti di dati interessati: sono indicati i trattamenti di dati, sensibili e giudiziari, effettuati nell'ambito della predetta attività.

Soggetto esterno: è indicata la società, l'ente o il consulente cui è stata affidata l'attività.

Tabella 1 – Trattamenti affidati all'esterno

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno
Vedi atti di nomina		

PARTE III

MISURE DI SICUREZZA
E PRESCRIZIONI PER IL 2015

PREMESSA

Il documento intende essere uno strumento operativo che permetta al Comune di avere una rappresentazione delle misure minime di sicurezza e delle prescrizioni che risultano ancora da realizzare.

MISURE E PRESCRIZIONI GIURIDICO-ORGANIZZATIVE:

Sono adottati i seguenti Adempimenti privacy	Si	No	Annotazioni
Nomina responsabili e incaricati interni	X		Da rivedere
Nomina responsabili e incaricati esterni	X		Da rivedere
Nomina amministratore/i di sistema	X		Da rivedere
Informativa ai sensi dell'art. 13 D.lgs. 196/2003	X		
Informativa ai sensi degli artt. 13 e 22 D.lgs. 196/2003	X		
Regolamento privacy		X	
Regolamento per il trattamento dei dati sensibili e giudiziari	X		
Regolamento dell'informazione sull'attività comunale attraverso la rete civica comunale e di gestione dell'albo pretorio	X		
Attività di videosorveglianza	X		
Disciplinare per l'utilizzo di internet e della posta elettronica	X		
Documento programmatico privacy	X		
Formazione del personale	X		
Sicurezza fisica			
Profili di autorizzazione	X		
Corretta gestione custodia di atti e documenti	X		
Archivi ad accesso selezionato	X		
Identificazione e registrazione di persone non incaricate del trattamento dopo l'orario di chiusura	X		

IMPLEMENTAZIONE MISURE GIURIDICO – ORGANIZZATIVE

Da rivedere la documentazione relativa agli atti di nomina

Formazione per il personale

MISURE DI SICUREZZA INFORMATICHE

Misure minime di sicurezza – Trattamenti con strumenti elettronici – sono adottate le misure?	Si	No	Annotazioni
Sistema di autenticazione informatica			
Credenziali di autenticazione	X		
Istruzioni agli incaricati per la corretta gestione delle credenziali di autenticazione	X		
Procedure di gestione delle credenziali di autenticazione	X		
Sistema di autorizzazione			
Creazione profili di autorizzazione	X		
Verifica periodica dei profili di autorizzazione	X		
Sistema idoneo alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema	X		
Altre misure di sicurezza informatiche			
Protezione degli strumenti e dei dati rispetto a trattamenti illeciti, accessi non consentiti (interni ed esterni) e a programmi informatici	X		
Aggiornamento semestrale degli strumenti di protezione	X		
Custodia di copie di sicurezza con salvataggio settimanale dei dati	X		
Procedure di ripristino della disponibilità dei dati e dei sistemi	X		
Formazione del personale	X		

IMPLEMENTAZIONE MISURE DI SICUREZZA INFORMATICHE