COMUNE DI TRENTO

DIRETTIVE PER IL TRATTAMENTO DEI DATI PERSONALI

versione:	3.0
data:	28.04.2025
redatto da:	Segreteria generale
rivisto da:	Servizio innovazione e transizione digitale
approvato da:	Giunta comunale

Cronologia delle revisioni

Versione	Data	Descrizione
1.0	15.07.2019	Prima approvazione
2.0	23.12.2024	Seconda approvazione
3.0	28.04.2025	Terza approvazione

INDICE

PREMESSA

Il presente documento stabilisce le direttive da seguire per il trattamento di dati personali effettuato nell'ambito del Comune di Trento, in applicazione delle disposizioni del Regolamento UE n. 2016/679 e del decreto legislativo n. 196/2003.

A tal fine il presente documento:

- richiama le fonti normative in materia di trattamento di dati personali vigenti a livello europeo, nazionale e comunale;
- definisce i ruoli e le responsabilità spettanti ai soggetti operanti nell'ambito del Comune di Trento con riferimento al trattamento dei dati personali;
- individua gli obblighi da osservare e gli adempimenti da porre in essere nell'ambito del Comune di Trento ai fini del rispetto della normativa vigente in materia di trattamento di dati personali;
- individua le misure di sicurezza da applicare al trattamento di dati personali effettuato nell'ambito del Comune di Trento.

Il presente documento è rivolto a ciascun dirigente e dipendente del Comune di Trento, ai fini della puntuale applicazione delle direttive da esso stabilite.

Il presente documento è approvato dalla Giunta comunale su proposta della Segreteria generale e del Servizio Innovazione e transizione digitale, che ne curano la redazione e l'aggiornamento.

1. QUADRO NORMATIVO E DEFINIZIONI

1.1. Quadro normativo

Normativa europea

- Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "GDPR").
  Il Regolamento è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 ed è entrato in vigore il 24 maggio 2016. Le disposizioni del Regolamento sono divenute direttamente applicabili negli Stati membri a decorrere dal 24 maggio 2018.
- Regolamento UE 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (di seguito "AI ACT").
  Il Regolamento è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 12 luglio 2024 ed è entrato in vigore il 1° agosto 2024. Le disposizioni del Regolamento diverranno completamente applicabili negli Stati membri a decorrere dal 2 agosto 2026.

Normativa nazionale

- Decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (di seguito "Codice").
- Decreto legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale" (di seguito "CAD");
- Decreto legislativo 4 settembre 2024, n. 138, "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148" (di seguito "Decreto cibersicurezza").

Normativa comunale

- Regolamento per la tutela della riservatezza dei dati personali (di seguito "regolamento comunale");
- Regolamento per l'utilizzo degli impianti di videosorveglianza (di seguito "regolamento videosorveglianza").

1.2. Definizioni

Dato personale
qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati particolari
dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale della persona, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati giudiziari
dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
Dati genetici
dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati biometrici
dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute
dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Trattamento di dati personali
qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Comunicazione di dati personali
il dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione o mediante interconnessione.

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

Violazione di dati personali
violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Interessato
la persona fisica a cui si riferiscono i dati personali.

Titolare del trattamento
la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Responsabile del trattamento
la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Designato al trattamento
la persona fisica, espressamente designata, che opera sotto la diretta autorità del titolare o del responsabile, alla quale sono attribuiti specifici compiti e funzioni connessi al trattamento di dati personali.

Autorizzato al trattamento
la persona fisica che tratta i dati personali sotto la diretta autorità del titolare, del designato o del responsabile e sulla base delle istruzioni dagli stessi impartite.

Amministratore di sistema
il soggetto che ha fra i suoi compiti anche quello di sovrintendere all'applicazione delle misure di sicurezza relative al trattamento di dati personali effettuato con strumenti elettronici o comunque automatizzati.

Referente informatico
il soggetto ausiliario per l'attuazione delle misure di sicurezza relative al trattamento di dati personali effettuato con strumenti elettronici o comunque automatizzati.

2. SOGGETTI E RUOLI

2.1. Soggetti e ruoli interni al Comune di Trento

L'applicazione del GDPR rende necessaria l'attribuzione ai soggetti interni all'amministrazione comunale di specifici ruoli inerenti il trattamento di dati personali.
Nel presente paragrafo sono illustrate le modalità di definizione e di attribuzione di tali ruoli e sono stabiliti i compiti ad essi associati, anche in relazione al quadro delle responsabilità connesse al trattamento di dati personali (si rinvia in proposito al paragrafo 2.4.).
Con riferimento ai ruoli dei soggetti interni al Comune di Trento, si evidenzia in particolare che:

- ogni dirigente comunale, in qualità di *designato*, è responsabile del trattamento di dati personali effettuato in relazione all'ambito di attribuzioni, funzioni e competenze conferite, nel rispetto della normativa vigente e delle presenti direttive;
- ogni dipendente comunale, in qualità di *autorizzato*, è responsabile del trattamento di dati personali effettuato in relazione e per l'adempimento delle mansioni e dei compiti assegnati, nel rispetto della normativa vigente e delle presenti direttive.

2.1.1. TITOLARE DEL TRATTAMENTO

Ai sensi del GDPR è titolare del trattamento la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Titolare del trattamento di dati personali effettuato nell'ambito dell'amministrazione comunale è il Comune di Trento, rappresentato dal Sindaco in carica.

Funzioni del titolare del trattamento
Al titolare del trattamento competono in particolare le seguenti funzioni:

- definire i profili organizzativi e gestionali del trattamento di dati personali effettuato nell'ambito dell'amministrazione comunale, tramite emanazione di apposite direttive;
- definire i profili inerenti la sicurezza del trattamento di dati personali effettuato nell'ambito dell'amministrazione comunale, tramite emanazione di apposite direttive;
- nominare l'amministratore di sistema del Comune di Trento e vigilare sul suo operato;
- nominare i soggetti interni designati al trattamento di dati personali e vigilare sul loro operato;
- nominare i soggetti esterni responsabili del trattamento di dati personali e vigilare sul loro operato.

Per lo svolgimento di tali funzioni il Sindaco si avvale del supporto della Segreteria generale e del Servizio Innovazione e transizione digitale e del supporto fornito dal DPO (paragrafo 2.3.).

2.1.2. DIRIGENTI DESIGNATI AL TRATTAMENTO

Ai sensi del Codice è designato al trattamento la persona fisica che opera sotto la diretta autorità del titolare o del responsabile ed alla quale sono attribuiti specifici compiti e funzioni connessi al trattamento di dati personali.
Ogni dirigente comunale è nominato dal Sindaco quale designato al trattamento di dati personali effettuato nell'ambito delle attribuzioni, funzioni e competenze conferite.

Adempimenti operativi dei dirigenti designati al trattamento
Nei limiti delle attribuzioni, funzioni e competenze conferite, ogni dirigente comunale, in qualità di designato al trattamento, è responsabile dell'adozione dei seguenti adempimenti:

- sovraintendere al trattamento dei dati personali di competenza del proprio servizio o ufficio, come individuato nel registro delle attività di trattamento;
- verificare e garantire che il trattamento dei dati personali di competenza del proprio servizio o ufficio sia effettuato nel rispetto della normativa vigente in materia e delle direttive emanate dal titolare;
- rappresentare il titolare, per quanto di competenza del proprio servizio o ufficio, nella stipulazione degli atti di cui all'articolo 26 del GDPR, nella controfirma per accettazione degli atti di cui all'articolo 28 del GDPR e nella sottoscrizione degli ulteriori atti esecutivi adottati sulla base dello stesso;
- fungere da referente, per quanto di competenza del proprio servizio o ufficio, per la gestione delle violazioni dei dati personali, eseguendo gli opportuni controlli ed effettuando le necessarie segnalazioni (si rinvia in proposito alle istruzioni operative di cui al paragrafo 3.3.3.);
- fungere da referente, per quanto di competenza del proprio servizio o ufficio, per la mappatura dei trattamenti, per l'implementazione del registro delle attività di trattamento e per lo svolgimento della valutazione di impatto sulla protezione dei dati personali, curando i necessari aggiornamenti (si rinvia in proposito alle istruzioni operative di cui ai paragrafi 3.3.1. e 3.3.2.);
- proporre al titolare, per quanto di competenza del proprio servizio o ufficio, la stipulazione di accordi di contitolarità con soggetti esterni all'amministrazione comunale e la nomina di soggetti esterni all'amministrazione comunale a responsabili del trattamento (si rinvia in proposito alle istruzioni operative di cui ai paragrafi 2.2.2. e 2.2.3.);
- designare gli autorizzati al trattamento dei dati personali del proprio servizio o ufficio, curando la predisposizione e l'aggiornamento dei relativi atti di nomina e verificando periodicamente i relativi profili di autorizzazione (si rinvia in proposito alle istruzioni operative di cui ai paragrafi 2.1.3., 2.2.4., 4.1.1.2. e 4.2.1.1.);
- sulla base delle direttive emanate dal titolare, impartire agli autorizzati al trattamento del proprio servizio o ufficio le disposizioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati, eseguendo gli opportuni controlli;
- sulla base delle direttive emanate dal titolare, adottare le misure e disporre gli interventi ne-

cessari per la sicurezza del trattamento dei dati e per il corretto accesso ai dati (si rinvia in proposito alle istruzioni operative di cui al capitolo 4);
- curare l'informativa agli interessati, predisponendo la modulistica e altre forme idonee di informazione, inerenti al proprio servizio o ufficio (si rinvia in proposito alle istruzioni operative di cui al paragrafo 3.2.1.);
- collaborare con il titolare per l'evasione delle richieste di esercizio dei diritti degli interessati e delle istanze del Garante per la protezione dei dati personali (si rinvia in proposito alle istruzioni operative di cui al paragrafo 3.2.2.);
- fare la ricognizione delle banche dati esistenti nel proprio servizio o ufficio con tutti gli elementi necessari per la loro precisa identificazione, sulla base delle istruzioni fornite dalle competenti strutture comunali;
- sovrintendere ai procedimenti di comunicazione, diffusione, trasformazione, blocco, aggiornamento, rettificazione, integrazione e cancellazione dei dati;
- accedere ai soli dati personali la cui conoscenza sia strettamente necessaria in relazione all'ambito di attribuzioni, funzioni e competenze conferite;
- accedere esclusivamente agli applicativi informatici ed alle banche dati informatiche e cartacee il cui utilizzo è necessario per lo svolgimento delle attribuzioni, funzioni e competenze conferite.

2.1.3. DIPENDENTI AUTORIZZATI AL TRATTAMENTO

Ai sensi del GDPR è autorizzato al trattamento la persona fisica che tratta i dati personali sotto la diretta autorità del titolare, del designato o del responsabile e sulla base delle istruzioni dagli stessi impartite.
Ciascun dipendente comunale è nominato dal proprio dirigente quale autorizzato al trattamento di dati personali necessario in relazione e per l'adempimento delle mansioni e dei compiti assegnati. La nomina è formalizzata, con riferimento a singoli dipendenti o a gruppi di dipendenti, sulla base di apposito modello (allegato 2.2.C).

Adempimenti operativi dei dipendenti autorizzati al trattamento
Nei limiti delle mansioni e dei compiti assegnati, ogni dipendente comunale, in qualità di autorizzato al trattamento, è responsabile dei seguenti adempimenti:
- effettuare il trattamento nel rispetto della normativa vigente in materia di protezione dei dati personali, attenendosi alle istruzioni operative impartite dal dirigente designato sulla base delle direttive emanate dal titolare;
- accedere esclusivamente ai dati personali a cui è stato autorizzato dal dirigente designato e la cui conoscenza è strettamente necessaria in relazione e per l'adempimento delle mansioni e dei compiti assegnati;
- accedere esclusivamente agli applicativi informatici ed alle banche dati informatiche e cartacee a cui è stato autorizzato dal dirigente designato ed il cui utilizzo è strettamente necessario in relazione e per l'adempimento delle mansioni e dei compiti assegnati;

- non trasmettere o comunicare a soggetti terzi non legittimati e non diffondere illegittimamente i dati personali a cui è autorizzato ad accedere per l'adempimento delle mansioni e dei compiti assegnati;
- trattare i dati personali a cui è autorizzato ad accedere per il tempo strettamente necessario all'adempimento delle mansioni e dei compiti assegnati;
- adottare, nello svolgimento delle mansioni e dei compiti assegnati, le misure e gli interventi per la sicurezza del trattamento dei dati e per la correttezza dell'accesso ai dati, disposti dal dirigente designato sulla base delle direttive emanate dal titolare (si rinvia in proposito alle istruzioni operative di cui al capitolo 4);
- conservare gli atti e i documenti affidati per esigenze di servizio, secondo le disposizioni impartite dal dirigente designato sulla base delle direttive emanate dal titolare (si rinvia in proposito alle istruzioni operative di cui al paragrafo 4.2.2.);
- fornire, nei casi previsti dalla normativa vigente in materia di protezione dei dati personali, l'informativa agli interessati (si rinvia in proposito alle istruzioni operative di cui al paragrafo 3.2.1.);
- segnalare al dirigente designato eventuali violazioni di dati personali di cui abbia avuto conoscenza, sulla base delle direttive emanate dal titolare (si rinvia in proposito alle istruzioni operative di cui al paragrafo 3.3.3.).

2.1.4. RESPONSABILE DELLA TRANSIZIONE AL DIGITALE

Ai sensi del CAD, il responsabile della transizione al digitale ha il compito di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività.
Il dirigente del Servizio Innovazione e transizione digitale è nominato dal Sindaco quale responsabile della transizione al digitale del Comune di Trento.

2.1.5. RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

Il responsabile dell'intelligenza artificiale ha il compito di promuovere e coordinare gli interventi per l'implementazione dell'intelligenza artificiale nell'ambito dell'amministrazione comunale e di promuovere un sistema di verifica della conformità dei sistemi di intelligenza artificiale introdotti con la normativa vigente in materia di protezione dei dati personali e di sicurezza cibernetica.
Il dirigente del Servizio Innovazione e transizione digitale è nominato dal Sindaco quale responsabile dell'intelligenza artificiale del Comune di Trento.

2.1.6. AMMINISTRATORE DI SISTEMA

Ai sensi del regolamento comunale, è amministratore di sistema il soggetto che sovrintende all'applicazione delle misure di sicurezza relative al trattamento dei dati personali effettuato con strumenti elettronici o comunque automatizzati.
Il dirigente del Servizio Innovazione e transizione digitale è nominato dal Sindaco quale amministratore di sistema del Comune di Trento.

Il dirigente del Servizio Innovazione e transizione digitale nomina a sua volta gli amministratori di sistema tra i propri dipendenti.

2.1.7. REFERENTI INFORMATICI

Ai sensi del regolamento comunale, è referente informatico il soggetto ausiliario per l'attuazione delle misure di sicurezza relative al trattamento di dati personali effettuato con strumenti elettronici o comunque automatizzati.
Ogni dirigente comunale nomina uno o più referenti informatici tra i propri dipendenti. Le nomine sono formalizzate sulla base di apposito modello (allegato 2.2.E) e comunicate alla Segreteria generale che aggiorna l'elenco dei referenti informatici.
I compiti del referente informatico sono:

- collaborare con il dirigente designato nel disporre ed adottare le misure e gli interventi per la sicurezza del trattamento dei dati e per la correttezza dell'accesso ai dati, sulla base delle disposizioni della normativa vigente in materia di protezione dei dati personali e delle direttive emanate dal titolare;
- fornire agli autorizzati del proprio servizio o ufficio il supporto e le informazioni necessarie per il sicuro trattamento dei dati personali;
- segnalare tempestivamente al dirigente designato eventuali problemi riscontrati con riferimento all'adozione e applicazione delle misure e degli interventi per la sicurezza del trattamento dei dati e per la correttezza dell'accesso ai dati;
- partecipare ai corsi di formazione organizzati dall'amministrazione comunale.

2.2. Soggetti e ruoli esterni al Comune di Trento

L'amministrazione comunale, nello svolgimento delle proprie funzioni istituzionali, si avvale dell'attività di soggetti terzi. In tali casi, ai sensi del GDPR, occorre definire la natura dei rapporti reciproci e, se necessario, disciplinare in appositi atti i compiti e le responsabilità connessi al trattamento di dati personali.
Sulla base del GDPR, ai soggetti esterni all'amministrazione comunale possono essere attribuiti i seguenti ruoli:

- autonomi titolari del trattamento;
- contitolari del trattamento;
- responsabili del trattamento;
- autorizzati al trattamento.

Nel presente paragrafo si forniscono pertanto le istruzioni operative necessarie all'individuazione dei ruoli dei soggetti esterni all'amministrazione comunale ed alla gestione dei relativi rapporti, sulla base delle disposizioni dettate in proposito dal GDPR.
A tal riguardo, in applicazione dei principi della *privacy by design e by default* di seguito richiamati (paragrafo 3.1.1.2.), si rileva l'esigenza che le valutazioni necessarie all'individuazione dei ruoli dei

soggetti esterni all'amministrazione comunale ed alla gestione dei relativi rapporti siano svolte – ove necessario con il supporto della Segreteria generale e del Servizio Innovazione e transizione digitale – fin dalle fasi di programmazione e di progettazione delle rispettive attività, in modo da consentire la tempestiva attuazione degli adempimenti eventualmente necessari sulla base del GDPR e del Codice. Si richiama in proposito la responsabilità dei dirigenti in qualità di designati al trattamento per l'ambito di attribuzioni, funzioni e competenze conferite.

2.2.1. AUTONOMI TITOLARI DEL TRATTAMENTO

Sono qualificabili come autonomi titolari i soggetti terzi che trattano dati di cui è titolare anche il Comune di Trento, per finalità diverse o ulteriori rispetto a quelle perseguite dal Comune stesso ai fini dello svolgimento delle proprie funzioni istituzionali.
Rientrano in tale qualifica i soggetti terzi che collaborano con il Comune di Trento per lo svolgimento di attività delle quali determinano autonomamente obiettivi e mezzi strumentali.

Adempimenti operativi
I rapporti tra il Comune di Trento ed i soggetti terzi autonomi titolari del trattamento non necessitano di disciplina, essendo tali soggetti autonomamente vincolati al rispetto della normativa vigente in materia di protezione dei dati personali.
Peraltro, nei casi in cui i rapporti con tali soggetti comportano il trattamento di dati personali, è opportuno inserire nei relativi contratti apposita clausola (allegato 2.2.A)

2.2.2. CONTITOLARI DEL TRATTAMENTO

Sono qualificabili come contitolari i soggetti terzi che trattano dati personali di cui è titolare anche il Comune di Trento, determinando congiuntamente al Comune stesso le finalità ed i mezzi del trattamento.
Rientrano in tale qualifica i soggetti terzi che collaborano con il Comune di Trento per lo svolgimento di attività che implicano la condivisione di obiettivi e mezzi strumentali (a titolo esemplificativo: soggetti convenzionati con il Comune di Trento per la gestione associata di funzioni).

Adempimenti operativi
Ai sensi del GDPR, i rapporti tra contitolari del trattamento sono disciplinati in appositi accordi, con i quali sono in particolare stabiliti:

- le modalità di esercizio dei diritti degli interessati;
- le modalità dell'informativa agli interessati;
- le misure tecniche ed organizzative da applicare al trattamento;
- gli ulteriori diritti ed obblighi reciproci dei contitolari del trattamento per il rispetto delle disposizioni del GDPR.

Ai fini del rispetto di tali disposizioni, spettano ai dirigenti designati – con riferimento all'ambito di attribuzioni, funzioni e competenze rispettivamente conferite – i seguenti adempimenti:

- individuazione delle ipotesi di contitolarità del trattamento;

- segnalazione scritta alla Segreteria generale delle ipotesi di contitolarità del trattamento individuate;
- collaborazione con la Segreteria generale per la predisposizione degli schemi di accordo di contitolarità del trattamento;
- formalizzazione degli accordi di contitolarità del trattamento in appositi contratti, ovvero in appositi allegati dei contratti a cui i rapporti di contitolarità si riferiscono previo inserimento nei contratti stessi di apposita clausola (allegato 2.2.A)

2.2.3. RESPONSABILI DEL TRATTAMENTO

Sono qualificabili come responsabili i soggetti terzi che trattano dati personali per conto del titolare Comune di Trento, al quale solo restano riservate le decisioni in merito alle finalità ed ai mezzi del trattamento.
Rientrano in tale qualifica i soggetti terzi che svolgono per conto del Comune di Trento attività di cui il Comune stesso stabilisce obiettivi e mezzi strumentali e rispetto alle quali impartisce istruzioni ed effettua controlli (a titolo esemplificativo: appaltatori).

Adempimenti operativi
Ai sensi del GDPR, i rapporti tra titolari e responsabili del trattamento sono disciplinati in appositi atti giuridici, con i quali sono in particolare stabiliti:

- la durata del trattamento;
- la natura e le finalità del trattamento;
- i tipi di dati personali trattati;
- le categorie di interessati;
- il ricorso a sub-responsabili del trattamento;
- le istruzioni inerenti il trattamento dei dati personali;
- le misure tecniche ed organizzative da applicare al trattamento;
- gli ulteriori diritti ed obblighi reciproci del titolare e del responsabile del trattamento per il rispetto delle disposizioni del GDPR.

Ai fini del rispetto di tali disposizioni, spettano ai dirigenti designati – con riferimento all'ambito di attribuzioni, funzioni e competenze rispettivamente conferite – i seguenti adempimenti:

- individuazione delle ipotesi di responsabilità del trattamento;
- richiesta scritta alla Segreteria generale di predisposizione degli atti di nomina dei responsabili del trattamento individuati, corredata dall'indicazione degli elementi previsti dal GDPR come contenuti obbligatori degli atti di nomina e dall'indicazione delle misure di sicurezza da applicare al trattamento in relazione all'attività affidata al responsabile;
- formalizzazione degli atti di nomina dei responsabili del trattamento:
  - nei bandi, nei disciplinari o nei capitolati di gara, inserendo apposita clausola (allegato 2.2.A) e allegando schema dell'atto di nomina (allegato 2.2.B);
  - nei contratti, inserendo apposita clausola (allegato 2.2.A) ed allegando atto di nomina firmato dal Sindaco;

    - nei casi in cui non si procede all'esperimento di gare o alla stipulazione di contratti, tramite trasmissione degli atti di nomina sottoscritti dal Sindaco ai soggetti terzi, i quali devono restituirne copia debitamente controfirmata;
- monitoraggio sull'attività svolta dai responsabili nominati, mediante richiesta agli stessi, con cadenza almeno annuale, di relazioni scritte sui trattamenti di dati personali effettuati e sulle misure di sicurezza agli stessi applicate.

2.2.4. SOGGETTI ESTERNI AUTORIZZATI AL TRATTAMENTO

Sono qualificabili come autorizzati i soggetti esterni all'amministrazione comunale che trattano dati personali di cui essa è titolare sotto la diretta autorità dei dirigenti designati e sulla base delle istruzioni dagli stessi impartite.
Rientrano in tale qualifica, a titolo esemplificativo, i seguenti soggetti:

- lavoratori socialmente utili;
- lavoratori del "progettone";
- tirocinanti, stagisti e studenti;
- volontari del servizio civile.

Adempimenti operativi
Ognuno dei soggetti sopra indicati è nominato dal dirigente competente quale autorizzato al trattamento di dati personali necessario in relazione e per l'adempimento delle mansioni e dei compiti assegnati. La nomina è formalizzata sulla base di apposito modello (allegato 2.2.D).

2.3. Responsabile della protezione dei dati personali (DPO)

2.3.1. DESIGNAZIONE DEL DPO

Ai sensi del GDPR, il DPO:

- è designato obbligatoriamente se il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;
- è designato in funzione delle qualità professionali e della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali;
- può essere un dipendente del titolare del trattamento oppure assolvere i suoi compiti in base ad un contratto di servizi;
- opera in posizione di autonomia e di indipendenza nei confronti del titolare del trattamento.

In attuazione di tali disposizioni, il Comune di Trento ha affidato al Consorzio dei comuni trentini il servizio di Responsabile della protezione dei dati personali.
I dati di contatto del DPO sono pubblicati in apposita pagina del sito internet comunale.

2.3.2. COMPITI DEL DPO

Ai sensi del GDPR, al DPO spettano i seguenti compiti:

- informare e fornire consulenza al titolare del trattamento ed ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dal Codice;
- sorvegliare l'osservanza del GDPR, del Codice e delle direttive emanate dal titolare del trattamento in materia di protezione dei dati personali;
- fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- fungere da punto di contatto per gli interessati;
- fungere da punto di contatto e cooperare con l'Autorità di controllo.

Al Consorzio dei comuni trentini, in qualità di DPO del Comune di Trento, sono attribuiti specifici compiti di supporto all'amministrazione comunale in materia di protezione dei dati personali, riconducibili a quelli sopra indicati.

2.3.3. GRUPPO DI LAVORO INTERNO DI SUPPORTO AL DPO

Per garantire al DPO adeguato supporto organizzativo, opera un gruppo di lavoro interno all'amministrazione comunale composto da funzionari della Segreteria generale e del Servizio innovazione e transizione digitale, per il cui dettaglio si rinvia ad apposita pagina del sito internet comunale.
Tale gruppo di lavoro funge da punto di raccordo tra la struttura comunale e il DPO. Ad esso è necessario fare riferimento per qualsiasi esigenza connessa all'applicazione della normativa in materia di protezione dei dati personali nell'ambito dell'amministrazione comunale.

2.4. Responsabilità e sanzioni

Nel presente paragrafo si illustrano le responsabilità stabilite dal GDPR e dal Codice con riferimento al trattamento dei dati personali ed il relativo quadro sanzionatorio.
In relazione a quanto illustrato nel presente paragrafo, si richiama l'attenzione dei dirigenti designati e dei dipendenti autorizzati sull'esigenza di effettuare il trattamento di dati personali nel puntuale rispetto della normativa vigente e delle presenti direttive, in modo da prevenire possibili responsabilità e sanzioni a carico dell'amministrazione comunale e dei soggetti all'interno della stessa operanti.

2.4.1. RESPONSABILITÀ

Il GDPR ed il Codice prevedono le seguenti forme di responsabilità connesse al trattamento di dati personali:

- responsabilità civile
  comporta l'obbligo di risarcimento dei danni causati a terzi da violazioni del GDPR o del Codice, salva prova della non imputabilità dell'evento dannoso;
- responsabilità amministrativa
  comporta l'obbligo di pagamento delle sanzioni pecuniarie stabilite per le violazioni del GDPR o del Codice riguardanti tra l'altro:
  - i principi di base e le regole del trattamento;

  - i diritti degli interessati;
  - la definizione dei ruoli delle parti (accordi tra contitolari e nomine di responsabili);
  - la tenuta del registro delle attività di trattamento;
  - la cooperazione con l'Autorità di controllo;
  - l'applicazione di misure di sicurezza;
  - le violazioni di dati personali (*data breach*);
  - la valutazione di impatto sulla protezione dei dati personali e la consultazione preventiva dell'Autorità di controllo;
  - la nomina del responsabile della protezione dei dati (DPO);
- <u>responsabilità penale</u>
  sussiste in relazione agli illeciti penali in materia di trattamento di dati personali espressamente previsti dagli artt. 167-172 del Codice.

Ai sensi del GDPR e del Codice, le suddette forme di responsabilità si applicano ai diversi soggetti coinvolti nel trattamento di dati personali nei termini di seguito indicati:

- il titolare del trattamento risponde sul piano civile, amministrativo e penale di eventuali violazioni del GDPR o del Codice;
- i dirigenti designati e i dipendenti autorizzati al trattamento – rispettivamente per l'ambito di attribuzioni, funzioni e competenze conferite e per l'adempimento delle mansioni e dei compiti assegnati – rispondono sul piano civile, amministrativo e penale di eventuali violazioni del GDPR o del Codice;
- i contitolari del trattamento rispondono solidalmente sul piano civile, penale ed amministrativo di eventuali violazioni del GDPR o del Codice;
- i responsabili del trattamento rispondono sul piano civile ed amministrativo – anche in solido con il titolare – nei casi di inadempimento degli obblighi del GDPR ad essi specificamente diretti o di inosservanza delle istruzioni ad essi impartite dal titolare del trattamento.

2.4.2. SANZIONI

Il GDPR ed il Codice stabiliscono, in relazione alle forme di responsabilità connesse al trattamento di dati personali, il seguente regime sanzionatorio:

- <u>sanzioni civili</u>
  risarcimento del danno;
- <u>sanzioni amministrative</u>
  sanzioni pecuniarie fino a 20 milioni di euro. L'ammontare delle sanzioni pecuniarie applicabili nei singoli casi è determinato dall'Autorità di controllo sulla base dei criteri stabiliti dall'art. 83 del GDPR e dall'art. 166 del Codice;
- <u>sanzioni penali</u>
  sanzioni stabilite dagli artt. 167-172 del Codice.

3. OBBLIGHI E ADEMPIMENTI

3.1. Trattamento di dati personali

Ai sensi del GDPR è trattamento qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
La definizione dettata dal GDPR ha carattere esemplificativo e non esaustivo. Pertanto costituisce trattamento e rientra nel campo di applicazione del GDPR qualsiasi operazione compiuta sui dati personali, anche se non compresa tra quelle indicate nel sopra riportato elenco.
Al trattamento di dati personali devono essere applicati i principi e le regole indicati nel presente paragrafo. Si richiama a riguardo la responsabilità dei dirigenti in qualità di designati al trattamento per l'ambito di attribuzioni, funzioni e competenze conferite.

3.1.1. PRINCIPI APPLICABILI AL TRATTAMENTO

3.1.1.1. Principio di liceità

Il GDPR individua le seguenti condizioni di liceità del trattamento di dati personali:

- consenso dell'interessato;
- esecuzione di un contratto di cui l'interessato è parte o di misure precontrattuali adottate su richiesta dello stesso;
- adempimento di un obbligo legale a cui è soggetto il titolare del trattamento;
- salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- perseguimento del legittimo interesse del titolare del trattamento o di terzi.

La condizione di liceità del trattamento di dati personali da parte dell'amministrazione comunale è costituita dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Ai sensi del Codice la relativa base giuridica è costituita da una norma di legge o regolamento o da atti amministrativi generali.
Si evidenzia che il consenso dell'interessato - condizione di liceità generalmente rilevante nei rapporti tra privati - non costituisce valido presupposto per il trattamento di dati personali da parte dell'amministrazione comunale.

3.1.1.2. Principio di responsabilizzazione

Ai sensi del GDPR il titolare del trattamento è competente per il rispetto della normativa vigente in materia di protezione dei dati personali e deve essere in grado in comprovarlo.
Tale principio determina il passaggio da un sistema basato sull'adempimento di obblighi normati-

vamente predeterminati ad un sistema basato sull'attribuzione al titolare del trattamento del compito di individuare, attuare e documentare le misure necessarie al rispetto della normativa in materia di protezione dei dati personali.
In base a tale principio, competono al titolare del trattamento:

- la dimostrazione della concreta adozione delle misure necessarie a garantire il rispetto del GDPR *(accountability);*
- l'individuazione, a partire dalla fasi di programmazione e progettazione delle singole attività che comportano il trattamento di dati personali, delle misure necessarie a garantire il rispetto del GDPR e la tutela dei diritti degli interessati (*privacy by design*);
- l'adozione di misure finalizzate a garantire che siano raccolti, trattati e conservati esclusivamente i dati personali necessari per lo svolgimento delle singole attività (*privacy by default*).

Ne deriva che:

- ogni trattamento di dati personali effettuato nell'ambito dell'amministrazione comunale deve avvenire nel rispetto delle presenti direttive e di ogni altra istruzione emanata dal titolare;
- ogni trattamento di dati personali effettuato nell'ambito dell'amministrazione comunale deve essere preceduto da una specifica analisi volta ad individuare e programmare le misure necessarie al rispetto della normativa vigente, delle presenti direttive e di ogni altra istruzione emanata dal titolare. A tale analisi provvedono – ove necessario con il supporto della Segreteria generale e del Servizio Innovazione e transizione digitale – i dirigenti designati al trattamento per l'ambito di attribuzioni, funzioni e competenze rispettivamente conferite;
- ogni trattamento di dati personali effettuato nell'ambito dell'amministrazione comunale è ammesso unicamente nei limiti in cui è necessario per lo svolgimento di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri di cui essa è investita. A sua volta, il trattamento di dati personali da parte di singoli dirigenti e dipendenti comunali è ammesso unicamente nei limiti in cui è necessario rispettivamente per la gestione delle attribuzioni, funzioni e competenze conferite e per lo svolgimento delle mansioni e dei compiti assegnati.

Al fine di garantire attuazione al principio di responsabilizzazione e ai criteri della *privacy by design* e *by default*, è prescritto l'utilizzo, fin dalle fasi di programmazione e di progettazione di qualsiasi attività che comporti il trattamento di dati personali, di apposita check list allegata alla presenti direttive (allegato 3.1.A). È inoltre prescritto lo svolgimento delle analisi di rischio ai sensi di quanto previsto dal paragrafo 3.3.2.

3.1.1.3. Principi di necessità, pertinenza e non eccedenza

Ai sensi del GDPR i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
Ne deriva che, con riferimento a ciascuna attività svolta nell'ambito dell'amministrazione comunale, il trattamento di dati personali è ammesso unicamente con riferimento ai dati necessari, pertinenti e non eccedenti in relazione alle finalità perseguite nei singoli casi.
Si rileva pertanto la necessità di astenersi dal raccogliere e conservare dati personali il cui trattamento non sia necessario in relazione alle singole attività, sulla base delle norme e delle prassi amministrative che ne regolano lo svolgimento.

3.1.1.4. Altri principi

Si indicano di seguito gli ulteriori principi dettati dal GDPR per il trattamento di dati personali.

Principio di limitazione della finalità
I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Un ulteriore trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali.
Le finalità del trattamento di dati personali da parte dell'amministrazione comunale sono indicate nel registro delle attività di trattamento. Si rinvia in proposito al paragrafo 3.3.1.

Principio di limitazione della conservazione
I dati personali sono conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali possono essere conservati per periodi più lunghi se trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Principio di integrità e riservatezza
I dati personali sono trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
Si richiamano in proposito le misure di sicurezza di cui al capitolo 4 e le eventuali ulteriori istruzioni emanate dal titolare in materia di sicurezza.

Principio di correttezza e trasparenza
I dati personali sono trattati in modo corretto e trasparente nei confronti dell'interessato.

Principio di esattezza
i dati personali sono esatti e, se necessario, aggiornati.

3.1.2. REGOLE APPLICABILI AL TRATTAMENTO

3.1.2.1. Comunicazione di dati personali

Ai sensi del Codice è comunicazione il dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione o mediante interconnessione.
Il Codice prevede una disciplina differenziata rispettivamente per:

- la comunicazione di dati personali tra titolari che effettuano il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, la quale è ammessa se prevista da norme di legge o regolamento o da atti amministrativi generali, o

se comunque necessaria per lo svolgimento di di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri di cui è investito il richiedente;

- la comunicazione di dati personali da parte di titolari che effettuano il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri a soggetti che effettuano il trattamento per altre finalità, la quale è ammessa unicamente se prevista da norme di legge o regolamento.

La comunicazione di dati personali deve avvenire nel rispetto delle regole stabilite dal Garante per la protezione dei dati personali in apposito provvedimento.

Adempimenti operativi

Salvo quanto stabilito al paragrafo 3.1.2.3., sono stabilite le seguenti regole per la comunicazione di dati personali a soggetti esterni all'amministrazione comunale:

- la comunicazione a soggetti che effettuano il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (tipicamente altre pubbliche amministrazioni o gestori di pubblici servizi) è ammessa sulla base di apposita norma del regolamento comunale. Tale comunicazione può pertanto avvenire:
  - previa presentazione di richiesta scritta e motivata, se necessaria per lo svolgimento di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri di cui è investito il richiedente;
  - nel rispetto dei principi di necessità, pertinenza e non eccedenza applicabili al trattamento (paragrafo 3.1.1.3.);
- la comunicazione a soggetti che effettuano il trattamento per finalità diverse dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (tipicamente i soggetti privati) è ammessa unicamente se prevista da norme di legge o di regolamento. Tale comunicazione può pertanto avvenire:
  - se prevista dalle normative di settore;
  - nel rispetto dei principi di necessità, pertinenza e non eccedenza applicabili al trattamento (paragrafo 3.1.1.3.);

Non costituiscono comunicazione e non sono pertanto assoggettati alle regole sopra stabilite:

- lo scambio di dati personali tra strutture interne all'amministrazione comunale;
- lo scambio di dati personali tra titolare, responsabili, designati e autorizzati al trattamento.

3.1.2.2. Diffusione di dati personali

Ai sensi del Codice è diffusione il dare conoscenza di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. La diffusione è tipicamente integrata dalla pubblicazione in internet di dati personali.

Ai sensi del Codice la diffusione di personali è ammessa se prevista da norme di legge o regolamento o da atti amministrativi generali. È inoltre espressamente vietata la diffusione di dati biometrici, genetici e relativi alla salute.

Ai sensi del combinato disposto del Codice e della normativa in materia di trasparenza, la diffusione di dati personali tramite internet è ammessa unicamente se prevista da norme di legge o di re-

golamento.
La diffusione di dati personali deve avvenire nel rispetto delle regole stabilite dal Garante per la protezione dei dati personali in apposito provvedimento e in apposita pagina web informativa.

Adempimenti operativi
Salvo quanto stabilito al paragrafo 3.1.2.3., sono stabilite le seguenti regole per la diffusione di dati personali da parte dell'amministrazione comunale:

- la ***diffusione di dati personali tramite internet*** (siti web istituzionali e profili di social network gestiti dall'amministrazione comunale) è ammessa unicamente se prevista da norme di legge o di regolamento, in mancanza delle quali essa è da ritenersi preclusa. La diffusione può pertanto avvenire:
  - con riferimento ai dati personali inseriti in atti e provvedimenti amministrativi (deliberazioni, determinazioni, ordinanze, decreti), nel rispetto delle istruzioni operative diramate con circolare della Segreteria generale n. 5/2025, alla quale si rinvia;
  - con riferimento ai dati personali inseriti in atti e documenti diversi da deliberazioni, determinazioni, ordinanze e decreti ed in altri contenuti testuali, video ed immagini, se espressamente prevista da disposizioni delle normative di settore applicabili o dal regolamento comunale;
- la ***diffusione di dati personali tramite canali diversi da internet*** (quali a titolo esemplificativo eventi o manifestazioni pubblici gestiti o patrocinati dall'amministrazione comunale) è ammessa se prevista da norme di legge o regolamento o da atti amministrativi generali, in mancanza dei quali essa è da ritenersi preclusa;
- la diffusione di dati personali, laddove ammessa ai sensi dei precedenti capoversi, è subordinata al rispetto delle seguenti prescrizioni:
  - la pubblicazione di contenuti testuali, video ed immagini avviene sotto la supervisione e la responsabilità dei dirigenti designati al trattamento per gli ambiti di rispettiva competenza;
  - la pubblicazione di contenuti testuali, video ed immagini deve avvenire per il tempo strettamente necessario al perseguimento delle finalità per le quali è effettuata e deve essere successivamente rimossa dai siti web istituzionali, dai profili di social network, dagli eventi e dalle manifestazioni gestiti dall'amministrazione comunale;
  - la pubblicazione di video ed immagini deve avvenire con modalità tali da limitare l'identificabilità degli interessati e quindi privilegiando immagini di spalle, di gruppo o riprese da debita distanza ed evitando per quanto possibile primi piani di volti. Tali modalità devono essere osservate in particolare in caso di pubblicazione di video e immagini relativi a minori, per i quali sono vietati i primi piani di volti;
  - la pubblicazione di video ed immagini deve avvenire previa acquisizione di espressa autorizzazione degli interessati in relazione alla tutela del diritto all'immagine, per la quale è fornito apposito modello (allegato 3.1.B). In caso di pubblicazione di video e immagini relativi a minori, l'autorizzazione deve essere acquisita dagli esercenti la potestà genitoriale;

- la diffusione è ammessa nel rispetto dei principi di necessità, pertinenza e non eccedenza di cui al paragrafo 3.1.1.3. Pertanto, anche nelle ipotesi in cui è prevista da norme di legge o regolamento o da atti amministrativi generali, la diffusione può avvenire unicamente con riferimento ai dati personali indispensabili in relazione alle finalità del trattamento.

3.1.2.3. Trattamento di dati particolari e dati giudiziari

Il GDPR e il Codice prevedono specifiche cautele per il trattamento di dati particolari e dati giudiziari.
In particolare il trattamento di dati particolari e giudiziari da parte dell'amministrazione comunale, generalmente vietato, è ammesso nei casi in cui è necessario per motivi di interesse pubblico. In tali casi il trattamento è ammesso se previsto da norme di legge o di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili ed i motivi di interesse pubblico rilevanti.
Adempimenti operativi
Sulla base della disciplina dettata dal GDPR e dal Codice, sono stabilite le seguenti regole per il trattamento di dati particolari e dati giudiziari nell'ambito dell'amministrazione comunale:

- il trattamento è ammesso nei casi e nei limiti indicati in apposite schede allegate al regolamento comunale, nelle quali sono specificati, con riferimento ai diversi settori di attività dell'amministrazione comunale, i tipi di dati che possono essere trattati e le operazioni che possono essere eseguite sugli stessi. Compete ai dirigenti designati, con riferimento all'ambito delle attribuzioni, funzioni e competenze rispettivamente conferite:
  - verificare che il trattamento sia svolto nel rispetto dei limiti indicati nelle citate schede;
  - segnalare alla Segreteria generale eventuali necessità di aggiornamento o integrazione delle suddette schede;
- il trattamento è subordinato al rispetto dei principi di necessità, pertinenza e non eccedenza (paragrafo 3.1.1.3.). Esso è pertanto ammesso esclusivamente con riferimento ai dati strettamente indispensabili in relazione alle finalità perseguite nei singoli casi concreti;
- il trattamento è subordinato al rispetto delle seguenti prescrizioni:
  - obbligo di custodire i documenti cartacei contenenti dati particolari e giudiziari separatamente dagli altri documenti, in busta chiusa all'interno di fascicoli protocollati;
  - obbligo di trattare e custodire i documenti informatici contenenti dati particolari e giudiziari:
    - ✔ all'interno del File Server, in unità di rete distinte da quelle contenenti altri documenti e ad accesso selezionato, nel rispetto delle regole indicate al paragrafo 4.1.1.2.;
    - ✔ all'interno del protocollo informatico PITRE, in documenti, fascicoli e trasmissioni contrassegnati come privati e come tali visibili al solo ruolo proprietario e ad accesso selezionato;
    - ✔ all'interno del sistema di posta elettronica e collaboration, esclusivamente in comunicazioni e condivisioni strettamente indispensabili ed effettuate previa specifica verifica dei destinatari, nonché nel rispetto delle regole indicate al paragrafo 3.1.2.1.;
  - divieto di diffondere in qualsiasi forma dati biometrici, genetici e relativi alla salute.

3.1.2.4. Trattamento di dati personali in modalità di lavoro agile (smart working)

Il disciplinare per il lavoro agile nel Comune di Trento, da ultimo approvato con deliberazione della Giunta comunale n. 75/2023, disciplina presupposti e modalità dello svolgimento della prestazione lavorativa da remoto nel Comune di Trento.

Istruzioni operative

Il personale comunale autorizzato allo svolgimento del lavoro agile è tenuto a rispettare gli obblighi di riservatezza e ad osservare le presenti direttive, evitando di comunicare, diffondere, divulgare o riferire a soggetti non autorizzati dati, informazioni e documenti di cui viene in possesso o a conoscenza per lo svolgimento da remoto della prestazione lavorativa.

Sono stabilite le seguenti istruzioni operative per il trattamento di dati personali in modalità di lavoro agile, effettuato rispettivamente con l'ausilio di strumenti informatici e di supporti cartacei.

- ***Trattamento con l'ausilio di strumenti informatici***

  Il personale comunale autorizzato allo svolgimento del lavoro agile accede da remoto ai servizi informatici del Comune di Trento (server e cartelle, applicativi informatici, posta elettronica e collaboration) nel rispetto delle seguenti istruzioni:
  - i servizi informatici sono utilizzati dal dipendente esclusivamente per rendere la prestazione lavorativa da remoto;
  - l'utilizzo dei servizi informatici da remoto spetta esclusivamente al dipendente. Pertanto le credenziali di autenticazione ai servizi informatici (username e password) sono personali e riservate e devono essere conservate e custodite dal dipendente con la massima diligenza, nel rispetto delle regole stabilite al paragrafo 4.1.1.1;
  - l'accesso ai servizi informatici da remoto può avvenire tramite strumenti di proprietà o in disponibilità del dipendente (PC fissi e portatili, tablet, smartphone, reti wi-fi, collegamenti ad internet). In tali casi le credenziali di autenticazione ai servizi informatici non devono essere memorizzate nello strumento utilizzato dal dipendente, tramite funzionalità che permettono di salvare la password per non doverla digitare nuovamente al successivo accesso. È quindi vietata la funzione di log-in automatico;
  - i documenti utilizzati per rendere la prestazione lavorativa da remoto non possono essere salvati su strumenti (PC fissi e portatili, tablet, smartphone o altri) o supporti removibili (chiavi USB o altri) di proprietà o in disponibilità del dipendente;
  - al termine della prestazione lavorativa o in caso di allontanamento anche temporaneo dallo strumento utilizzato per rendere la prestazione lavorativa, il dipendente è tenuto obbligatoriamente ad attivare il salvaschermo, oppure a chiudere il proprio account di accesso ai servizi informatici effettuando il log-out;
  - il dipendente che smarrisce le credenziali di autenticazione ai servizi informatici o rileva incidenti informatici o comportamenti anomali dei servizi informatici o degli strumenti utilizzati per rendere la prestazione lavorativa da remoto è tenuto a darne tempestiva comunicazione al proprio dirigente ed al personale del Servizio Innovazione e transizione digitale.

- ***Trattamenti con l'ausilio di supporti cartacei***
  Sono stabilite le seguenti istruzioni operative:
  - divieto di comunicare a soggetti non specificatamente autorizzati atti, documenti, dati e informazioni dei quali si viene a conoscenza nello svolgimento della prestazione lavorativa;
  - in caso di telefonate o videoconferenze su tematiche sensibili (che coinvolgano persone fisiche e relativi dati personali particolari o giudiziari), obbligo di ritirarsi in luogo non accessibile a familiari o soggetti terzi;
  - obbligo di mantenere in ordine la postazione lavorativa, evitando di lasciare incustoditi appunti, fascicoli e documenti contenenti dati personali e custodendo con cura eventuali stampe di materiale di lavoro;
  - qualora risulti necessario eliminare documenti contenenti dati personali, obbligo di sminuzzarli diligentemente.

3.1.2.5. Trattamento dei dati da videosorveglianza

Il trattamento dei dati personali acquisiti mediante utilizzo degli impianti di videosorveglianza di proprietà del Comune di Trento o da esso gestiti è disciplinato dal regolamento videosorveglianza e dagli atti dallo stesso richiamati, ai quali si rinvia.

3.2. Informativa e diritti degli interessati

3.2.1. INFORMATIVA

In caso di raccolta di dati personali deve essere resa agli interessati un'informativa contenente gli elementi espressamente indicati dal GDPR.
Il GDPR distingue a seconda che i dati personali siano o meno raccolti direttamente presso gli interessati. Nel primo caso l'informativa deve essere fornita al momento della raccolta dei dati. Nel secondo caso l'informativa deve essere fornita entro un termine ragionevole, ovvero entro un mese dalla raccolta dei dati o al momento della prima comunicazione agli interessati.
Ai sensi del GDPR l'informativa deve contenere i seguenti elementi:

- identità e dati di contatto del titolare del trattamento o del suo rappresentante;
- identità e dati di contatto del responsabile della protezione dei dati personali (DPO);
- categorie di dati personali oggetto di trattamento;
- finalità e base giuridica del trattamento;
- eventuali destinatari o categorie di destinatari dei dati personali;
- natura obbligatoria o facoltativa del trattamento ed eventuali conseguenze del mancato conferimento dei dati;
- periodo di conservazione dei dati personali;
- eventuale trasferimento all'estero dei dati personali;
- diritti degli interessati.

Adempimenti operativi

Sono stabilite le seguenti regole per l'informativa sul trattamento di dati personali da parte dell'amministrazione comunale:

- l'informativa è resa all'atto della raccolta dei dati personali o al momento della prima comunicazione agli interessati;
- l'informativa è resa in forma scritta. A tal fine l'informativa:
  - è allegata alla modulistica ed alla documentazione in uso presso l'amministrazione comunale, in tutti i casi in cui i relativi procedimenti comportano la raccolta ed il trattamento di dati personali;
  - è allegata alla documentazione in uso presso l'amministrazione comunale per l'affidamento di appalti di lavori, servizi e forniture, in tutti i casi in cui le relative procedure comportano la raccolta ed il trattamento di dati personali;
- se non già fornita ai sensi del punto che precede, è resa disponibile, con riferimento ai dati personali dei sottoscrittori, all'atto della stipulazione di contratti, patti, convenzioni, accordi di cui è parte l'amministrazione comunale;
- se non già fornita ai sensi dei punti che precedono, è resa disponibile in forma cartacea presso ciascuna struttura comunale, in tutti i casi di raccolta e trattamento di dati personali;
- l'informativa è predisposta sulla base di apposito modello (allegato 3.2.A). L'utilizzo di eventuali forme semplificate di informativa non esime dall'obbligo di fornire un'informativa completa di tutti gli elementi contenuti nel modello;
- l'informativa è resa con riferimento ai singoli procedimenti o processi nel cui contesto i dati personali sono raccolti o con riferimento a categorie omogenee di procedimenti o processi. Non è ammesso l'utilizzo di informative generiche per categorie eterogenee di procedimenti o processi;
- ciascuna struttura comunale è responsabile della predisposizione e dell'aggiornamento delle informative relative ai procedimenti o processi di propria competenza, nonché della coerenza tra le informazioni contenute rispettivamente nelle informative e nelle corrispondenti schede del registro delle attività di trattamento (paragrafo 3.3.1.).

3.2.2. DIRITTI DEGLI INTERESSATI

Ai sensi del GDPR ogni interessato ha diritto di:

- chiedere la conferma dell'esistenza o meno di dati personali che lo riguardano;
- ottenere la comunicazione in forma intelligibile dei dati personali che lo riguardano;
- conoscere l'origine dei dati personali, le finalità e modalità del trattamento, la logica applicata al trattamento se lo stesso è effettuato con l'ausilio di strumenti elettronici;
- ottenere la rettifica, la cancellazione, la limitazione, la trasformazione in forma anonima o il blocco dei dati personali trattati in violazione di legge;
- aggiornare, correggere o integrare i dati personali che lo riguardano;
- opporsi, per motivi legittimi, al trattamento dei dati personali;
- proporre reclamo al Garante per la protezione dei dati personali.

I suddetti diritti sono esercitati nei confronti del titolare del trattamento, il quale è tenuto a fornire riscontro agli interessati entro un mese dalla ricezione della richiesta. Tale termine può essere prorogato di due mesi in relazione alla complessità ed al numero delle richieste.
L'esercizio dei diritti degli interessati è gratuito, salva facoltà del titolare di addebitare un contributo spese ragionevole in caso di richieste manifestamente infondate o eccessive.

Adempimenti operativi
Al fine di garantire l'uniforme gestione delle richieste di esercizio dei diritti degli interessati nell'ambito dell'amministrazione comunale, sono stabilite le seguenti regole:

- ogni richiesta ricevuta dai dirigenti designati o dai dipendenti autorizzati al trattamento è trasmessa senza ritardo al Segretario generale, individuato dal regolamento comunale quale responsabile per l'esercizio dei diritti degli interessati. Il Segretario generale valuta ed evade le richieste, se necessario in collaborazione coi dirigenti designati al trattamento o coi soggetti esterni responsabili del trattamento;
- le informazioni e la modulistica inerenti l'esercizio dei diritti degli interessati sono consultabili in apposita scheda informativa disponibile sul sito internet comunale.

3.3. Altri obblighi e adempimenti

3.3.1. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Ai sensi del GDPR ciascun titolare tiene un registro delle attività di trattamento di dati personali svolte sotto la propria responsabilità.
Il registro contiene, con riferimento a ciascuna attività di trattamento, le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e del DPO;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- i trasferimenti all'estero di dati personali;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali;
- una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il registro delle attività di trattamento di dati personali svolte presso il Comune di Trento è contenuto in apposito applicativo informatico, nel quale sono consultabili le attività di trattamento di competenza di ciascuna struttura comunale individuate sulla base della mappatura dei processi organizzativi.
L'accesso all'applicativo è consentito al personale appositamente designato da ciascuna struttura comunale (elenco allegato 3.3.A). Le indicazioni per l'utilizzo dell'applicativo sono consultabili in apposito manuale (allegato 3.3.C).

Adempimenti operativi
Spettano ai dirigenti designati, con riferimento all’ambito di attribuzioni, funzioni e competenze ri-

spettivamente conferite, i seguenti adempimenti:

- verificare e segnalare alla Segreteria generale ed al Servizio Innovazione e transizione digitale l'esistenza di eventuali trattamenti di dati personali ulteriori rispetto a quelli indicati nel registro delle attività di trattamento;
- garantire, d'intesa con la Segreteria generale, l'implementazione ed il costante aggiornamento delle informazioni contenute nel registro delle attività di trattamento, nel rispetto delle indicazioni fornite in apposita guida (allegato 3.3.B);
- garantire la coerenza tra le informazioni contenute rispettivamente nel registro delle attività di trattamento e nelle informative rese agli interessati (paragrafo 3.2.1.).

3.3.2. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

Ai sensi del GDPR, quando un trattamento può comportare un rischio elevato per i diritti e le libertà degli interessati, il titolare effettua una valutazione di impatto del trattamento stesso sulla protezione dei dati personali. Il titolare consulta l'Autorità di controllo se le misure tecniche ed organizzative individuate per mitigare l'impatto del trattamento non sono ritenute sufficienti, in quanto residuano rischi elevati per i diritti e le libertà degli interessati.
La valutazione di impatto sulla protezione dei dati personali è espressione del principio di responsabilizzazione del titolare ed è svolta sulla base del registro delle attività di trattamento.
Ad esito della compilazione del registro delle attività di trattamento, il Comune di Trento ha provveduto ad effettuare le analisi di rischio relative alle singole attività indicate nel registro. Ad esito dell'effettuazione delle analisi di rischio, si è proceduto allo svolgimento delle valutazioni di impatto relative alle attività di trattamento che possono comportare un rischio elevato per i diritti e le libertà degli interessati.
Le analisi di rischio e le valutazioni di impatto effettuate dal Comune di Trento sono consultabili nell'applicativo informatico contenente il registro delle attività di trattamento di dati personali. Le analisi di rischio e le valutazioni di impatto sono periodicamente aggiornate.

Adempimenti operativi

Spettano ai dirigenti designati, con riferimento all'ambito di attribuzioni, funzioni e competenze rispettivamente conferite, i seguenti adempimenti:

- collaborare con la Segreteria generale ed il Servizio innovazione e transizione digitale per l'effettuazione delle analisi di rischio e delle valutazioni di impatto relative a nuovi trattamenti inseriti nel registro, nonché per l'aggiornamento periodico delle analisi di rischio e delle valutazioni di impatto relative ai trattamenti già presenti nel registro e per la relativa validazione e sottoscrizione;
- segnalare alla Segreteria generale e al Servizio innovazione e transizione digitale l'esigenza di aggiornamento o revisione delle analisi di rischio e delle valutazioni di impatto relative ai trattamenti presenti nel registro.

3.3.3. GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

Ai sensi del GDPR è violazione di dati personali (*data breach*) qualsiasi violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
A titolo esemplificativo, costituiscono violazioni di dati personali (*data breach*): l'accesso o l'acquisizione di dati da parte di terzi non autorizzati; il furto o la perdita di dispositivi informatici contenenti dati personali; la deliberata alterazione di dati personali; l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware; la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità; la divulgazione non autorizzata di dati personali.
In caso di violazione di dati personali, il GDPR prescrive al titolare i seguenti adempimenti:

- notifica della violazione all'Autorità di controllo entro 72 ore dal momento in cui se ne ha avuto conoscenza;
- comunicazione della violazione agli interessati;
- tenuta di un registro delle violazioni di dati personali.

Procedura operativa
È stabilita la seguente procedura di gestione delle violazioni di dati personali nell'ambito della amministrazione comunale:

- il dipendente autorizzato che ha notizia di qualsiasi possibile violazione di dati personali ha obbligo di darne immediata segnalazione al dirigente designato;
- il dirigente designato che riceve la comunicazione di cui al punto precedente o che ha comunque notizia di qualsiasi possibile violazione di dati personali ha obbligo di:
  - darne immediata segnalazione alla Segreteria generale e al Servizio Innovazione e transizione digitale;
  - adottare, d'intesa con la Segreteria generale e il Servizio Innovazione e transizione digitale, le misure di sicurezza eventualmente necessarie per attenuare le conseguenze delle violazioni occorse;
  - effettuare e documentare, in collaborazione con la Segreteria generale e il Servizio Innovazione e transizione digitale, una specifica indagine sugli aspetti organizzativi, informatici e legali delle violazioni occorse;
- la Segreteria generale, in collaborazione con il Servizio Innovazione e transizione digitale, ad esito della ricezione delle comunicazioni e dello svolgimento degli adempimenti di cui ai punti precedenti, comunica immediatamente al DPO le violazioni occorse, fornendo puntuale informazione sugli esiti delle misure eventualmente adottate e delle indagini effettuate;
- il DPO, ad esito della ricezione delle comunicazioni e informazioni di cui al punto precedente e dell'analisi delle fattispecie segnalate, formula ed invia alla Segreteria generale e al Servizio Innovazione e transizione digitale specifici pareri non vincolanti sulla sussistenza o meno di violazioni di dati personali e di probabili rischi per i diritti e le libertà delle persone fisiche coinvolte;
- la Segreteria generale, in collaborazione con il Servizio Innovazione e transizione digitale,

tenuto conto dei pareri formulati dal DPO:

- se ritiene non sussistere violazioni di dati personali archivia le segnalazioni;
- se ritiene sussistere violazioni di dati personali non comportanti un probabile rischio per i diritti e le libertà delle persone fisiche coinvolte, documenta le violazioni occorse in apposito registro;
- se ritiene sussistere violazioni di dati personali comportanti un probabile rischio per i diritti e le libertà delle persone fisiche coinvolte, documenta le violazioni occorse in apposito registro ed effettua la notifica all'Autorità di controllo;
- se ritiene sussistere violazioni di dati personali comportanti un elevato rischio per i diritti e le libertà delle persone fisiche coinvolte, documenta le violazioni occorse in apposito registro ed effettua la notifica all'Autorità di controllo e la comunicazione agli interessati.

Altri adempimenti operativi

Ai fini della adeguata gestione e documentazione delle violazioni di dati personali, sono stabiliti i seguenti ulteriori adempimenti:

- la Segreteria generale, con la collaborazione del Servizio Innovazione e transizione digitale, effettua le notifiche delle violazioni all'Autorità di controllo sulla base di apposito modello;
- la Segreteria generale, con la collaborazione del Servizio Innovazione e transizione digitale, documenta qualsiasi violazione di dati personali in apposito registro, nel quale sono indicati le circostanze della violazione, le sue conseguenze ed i provvedimenti adottati per porvi rimedio.

4. MISURE DI SICUREZZA

4.1. Misure per il trattamento con ausilio di strumenti informatici[1]

4.1.1. MISURE TECNICHE E ORGANIZZATIVE

4.1.1.1. Sistema di autenticazione

Il sistema di autenticazione è diretto a disciplinare l'accesso agli strumenti informatici esistenti nell'organizzazione del Comune di Trento.
L'accesso agli strumenti informatici è consentito unicamente ad autorizzati dotati di credenziali di autenticazione personali, costituite da un codice identificativo (*userID*), da una parola chiave riservata (*password*) e – in taluni casi – da un ulteriore codice OTP (*one time password*) rilasciato via SMS o App.
Le credenziali di autenticazione sono rilasciate dall'amministratore di sistema su richiesta scritta dei dirigenti designati effettuata mediante il sistema di ticketing.
Tramite il sistema di autenticazione, gli autorizzati accedono ai seguenti strumenti informatici:

- PC ed altre dotazioni informatiche (ad esempio smartphone e tablet);
- servizi informatici quali:
  - File Server collegati;
  - applicativi informatici esistenti nell'organizzazione del Comune di Trento;
  - posta elettronica e collaboration;
  - firma digitale remota.

L'accesso ai suddetti strumenti informatici avviene da postazioni di lavoro preventivamente individuate ed assegnate personalmente a ciascun autorizzato. L'accesso da postazioni diverse da quelle assegnate avviene esclusivamente in caso di esigenze di servizio preventivamente autorizzate dal dirigente designato.

Regole per la gestione delle credenziali di autenticazione
Sono stabilite le seguenti regole per la gestione delle credenziali di autenticazione:

- le credenziali di autenticazione sono strettamente personali e non sono condivise con altri utenti. Gli autorizzati evitano di utilizzare credenziali di altri utenti, anche se conosciute casualmente o fornite volontariamente;
- le password sono composte da almeno 8 caratteri e non contengono riferimenti agevolmente riconducibili all'autorizzato. Le password sono modificate dall'autorizzato al primo utilizzo e, successivamente, con cadenza almeno trimestrale. Ogni nuova password deve essere diversa dalle precedenti. Ciascun autorizzato adotta le cautele necessarie a garantire la segretezza delle proprie password.
- le credenziali di autenticazione sono disattivate se non utilizzate da almeno sei mesi o in

1 Con riferimento alle Misure minime di sicurezza ICT per le pubbliche amministrazioni di cui alla circolare n. 2/2017 dell'Agenzia per l'Italia digitale (AGID) si rinvia al documento protocollo n. 35585/2023.

caso di perdita della qualifica che consente all'autorizzato di accedere agli strumenti informatici (ad esempio in caso di cessazione o sospensione dell'attività lavorativa).

4.1.1.2. Sistema di autorizzazione

Il sistema di autorizzazione è diretto a disciplinare l'accesso alle banche dati informatiche e agli applicativi informatici esistenti nell'organizzazione del Comune di Trento.
Le autorizzazioni all'accesso alle banche dati informatiche e agli applicativi informatici sono rilasciate e modificate dall'amministratore di sistema su richiesta scritta dei dirigenti designati effettuata mediante il sistema di ticketing.
I dirigenti designati definiscono i profili di autorizzazione dei singoli autorizzati anteriormente all'inizio del trattamento, in modo da garantire che lo stesso sia svolto esclusivamente con riferimento ai dati necessari per lo svolgimento delle mansioni e dei compiti assegnati.
I dirigenti designati provvedono con cadenza almeno annuale alla verifica e – se necessario – alla revisione dei profili di autorizzazione dei singoli autorizzati.
I dirigenti designati definiscono i profili di autorizzazione con riferimento a singoli autorizzati o a gruppi di autorizzati.
I dirigenti designati definiscono i profili di autorizzazione con riferimento:

- alle banche dati informatiche esistenti nel File Server;
- agli applicativi informatici esistenti nell'organizzazione del Comune di Trento.

Sistema di autorizzazione per le banche dati informatiche esistenti nel File Server
Le autorizzazioni relative ai dipendenti di ciascun servizio comunale sono contenute in apposito prospetto (tabella in formato CSV scaricabile alla voce *allegato per il documento privacy*) annualmente verificato e – se necessario – revisionato dai dirigenti designati, con la collaborazione dei referenti informatici[2].
A seguito di autorizzazione, gli autorizzati hanno accesso alle seguenti risorse del File Server:

- *unità locali del computer (C:\ e D:\):* unità installate fisicamente sui PC. Per tali unità non è garantito il backup automatico dei dati. Tali unità non devono essere utilizzate per conservare dati personali;
- *unità di rete individuali (K:\):* unità accessibili unicamente ai singoli utenti autenticati, in modalità lettura e scrittura. Per tali unità è garantito il backup automatico dei dati. Tali unità devono essere utilizzate per conservare dati personali che non possono o non necessitano di essere condivisi con altri utenti;
- *unità di rete comuni (S:\ e L:\):* unità accessibili rispettivamente a tutti gli utenti dei singoli servizi/uffici (S:\) e a tutti gli utenti dell'amministrazione (L:\), in modalità lettura e scrittura, salva personalizzazione di profili di autorizzazione limitatamente alle cartelle di primo livello. Per tali unità è garantito il backup automatico dei dati. Tali unità sono utilizzate unicamente per condividere file, documenti e programmi rispettivamente all'interno dei singoli

2 Nel prospetto sono indicati, con riferimento a ciascun servizio o ufficio:
- le autorizzazioni all'accesso alle unità di rete comuni *S:* assegnate ai gruppi di utenti;
- gli utenti (dipendenti comunali) assegnati a ciascun gruppo.

servizi/uffici (S:\) e all'interno dell'amministrazione (L:\). Tali unità devono essere utilizzate per conservare esclusivamente dati personali che possono o necessitano di essere condivisi con altri utenti. I dati personali conservati sulle unità S:\ e L:\ devono essere cancellati al termine del loro utilizzo. L'unità L:\ non deve essere in alcun caso utilizzata per conservare dati particolari o giudiziari.

Sistema di autorizzazione per gli applicativi informatici

Le autorizzazioni relative ai dipendenti di ciascun servizio comunale sono contenute in apposito prospetto annualmente elaborato dal Servizio Innovazione e transizione digitale. Il prospetto è inviato ai dirigenti designati e da questi verificato e – se necessario – revisionato, con la collaborazione dei referenti informatici[3].

A seguito di autorizzazione, gli autorizzati hanno accesso agli applicativi informatici esistenti nell'organizzazione del Comune di Trento.

4.1.1.3. Sistema di backup

Il sistema di backup è volto a prevenire il rischio di perdita accidentale dei dati mediante salvataggio automatico dei dati medesimi su disco o su nastro.

Per i dati contenuti nei server e nel sistema di storage ridondato sono previsti backup giornaliero, settimanale, mensile e annuale su disco.

Per i dati contenuti nel sistema AS400 sono previsti backup giornaliero, mensile e annuale su nastro.

I backup giornalieri e settimanali sono conservati per 30 giorni. I backup mensili sono conservati per 2 anni. I backup annuali sono conservati per 5 anni.

I nastri dei backup sono conservati in armadi ignifughi ad accesso controllato. I backup giornalieri su disco sono cifrati e replicati in automatico quotidianamente su un server remoto dislocato presso la sede di Fondazione Bruno Kessler. .

Procedura di ripristino di dati accidentalmente persi

Il ripristino dei dati è richiesto, tramite il sistema di ticketing, agli amministratori di sistema indicando:

- nome dell'utente che ha perso il file;
- nome e posizione del/dei database o del/dei file persi;
- data richiesta della versione del/dei database o del/dei file da recuperare.

A seguito della richiesta, gli amministratori di sistema provvedono a recuperare i file disponibili nei backup su disco o su nastro e ad avvisare l'utente dell'avvenuto ripristino.

4.1.1.4. Sistema antivirus e antispam

Il sistema antivirus è volto a prevenire l'azione dei programmi aventi per scopo o per effetto il dan-

3 Nel prospetto è contenuto, con riferimento a ciascun servizio, l'elenco delle applicazioni informatiche accessibili da ciascun dipendente comunale.

neggiamento 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 (programmi comunemente noti come *virus*).
Il sistema antivirus è aggiornato quotidianamente e si basa su apposito software installato su tutti i PC dotati di sistema operativo Windows, sui server Windows e sui server Linux che espongono servizi di condivisione file. La gestione del sistema antivirus e dei relativi aggiornamenti è centralizzata ed automatica.
Il sistema antispam è volto a prevenire la ricezione di messaggi di posta elettronica indesiderati (messaggi comunemente noti come *spam*).
Il sistema antispam si basa su apposite tecniche automatiche di filtro della posta elettronica in entrata ed in uscita.

4.1.1.5. Sistema firewall

Il sistema firewall è volto a prevenire i rischi di intrusione e accesso non autorizzato agli strumenti informatici e ai dati in essi contenuti.
Il sistema firewall si basa su apposito software che garantisce la separazione tra la rete informatica comunale e le reti informatiche esterne (Internet e Telpat) e funge da strumento di controllo del traffico in entrata ed in uscita.

4.1.1.6. Sistema di monitoraggio dei server e della rete

Il sistema è volto a garantire il costante monitoraggio del funzionamento dei dispositivi e degli applicativi collegati alla rete informatica comunale.
Il sistema si basa su un apposito dispositivo hardware/software che consente il tempestivo rilevamento di malfunzionamenti o guasti dei dispositivi e degli applicativi monitorati.

4.1.2. MISURE DI SICUREZZA PER POSTA ELETTRONICA, INTERNET E TELEFONIA

4.1.2.1. Misure di sicurezza per posta elettronica ed internet

Le regole di utilizzo di posta elettronica e internet sono stabilite in apposito disciplinare a cui si rinvia.

4.1.2.2. Misure di sicurezza per i sistemi di telefonia fissa

Tutti gli utenti dotati di un telefono fisso connesso alla postazione di lavoro sono collegati alla rete internet tramite VOIP.
Ogni utente è direttamente responsabile dell'uso del telefono, dei soggetti che contatta, delle informazioni che fornisce all'interlocutore. Nell'utilizzo del telefono è necessario:

- qualificarsi all'interlocutore;
- accertarsi dell'identità dell'interlocutore prima di fornire informazioni o dati personali relativi ad una persona fisica.

L'utilizzo dei sistemi di telefonia fissa avviene nel rispetto delle disposizioni tecniche rese disponibili in apposita sezione di area intranet.

4.1.2.3. Misure di sicurezza per i sistemi di telefonia mobile

Le regole di assegnazione e di utilizzo di smartphone e tablet in dotazione ad amministratori, dirigenti e dipendenti comunali sono stabilite in apposito disciplinare al quale si rinvia.

4.1.3. MISURE LOGISTICHE E ORGANIZZATIVE

4.1.3.1. Misure di sicurezza per i server

Sono attuate misure di sicurezza volte a proteggere i server dai seguenti rischi:

- accesso fisico non autorizzato;
- distruzione o perdita di dati dovuta ad eventi fisici.

Gli amministratori di sistema ed i tecnici che hanno accesso ai locali in cui sono ospitati i server devono informare il dirigente del Servizio Innovazione e transizione digitale nel caso in cui riscontrino il mancato rispetto delle misure di sicurezza di seguito descritte.

Protezione dei server dal rischio di accesso fisico non autorizzato

Per tutelare la riservatezza dei dati presenti sui server e per preservare l'integrità delle apparecchiature, sono stabilite le seguenti misure di sicurezza:

- i server sono ospitati in appositi locali, destinati a contenere unicamente i server stessi ed eventualmente le apparecchiature di rete;
- i locali in cui sono ospitati i server, se situati in posizioni tali da rendere possibili intrusioni, sono muniti di adeguate protezioni, quali l'apposizione di sbarre alle finestre o altre;
- gli accessi ai locali in cui sono ospitati server sono chiusi a chiave. Le chiavi sono custodite da personale incaricato dal dirigente del Servizio Innovazione e transizione digitale. Il personale incaricato della custodia delle chiavi è tenuto a riporle in luoghi non agevolmente accessibili da altri;
- l'accesso ai locali in cui sono ospitati i server è consentito al personale del Servizio Innovazione e transizione digitale di seguito indicato: dirigente, amministratori di sistema, custodi delle chiavi, altro personale necessitato ad accedere per attività di gestione e manutenzione dei locali e delle apparecchiature o per altre attività indispensabili;
- l'accesso ai locali in cui sono ospitati i server da parte di personale non facente parte del Servizio Innovazione e transizione digitale è consentito esclusivamente in presenza del personale indicato al punto precedente. Gli interventi di manutenzione o di adeguamento dei locali e delle apparecchiature sono preventivamente autorizzati dal dirigente del Servizio Innovazione e transizione digitale. Le operazioni di pulizia dei locali in cui sono ospitati i server sono effettuate in date preventivamente programmate.

Protezione dei server dal rischio di distruzione o perdita di dati dovuta ad eventi fisici

Per prevenire i rischi di incendio, surriscaldamento e anomalia dell'alimentazione elettrica delle apparecchiature, sono stabilite le seguenti misure di sicurezza:

- in prossimità dei locali in cui sono ospitati i server è installato un dispositivo antincendio

munito di allarme;
- nei locali in cui sono ospitati i server è installato un sensore di temperatura che invia un'allerta al superamento di un valore soglia prestabilito (30° celsius);
- la cassette di backup sono custodite in armadi ignifughi;
- per garantire alimentazione elettrica ai server esistono due gruppi di continuità alimentati da una cabina elettrica di trasformazione. Esiste inoltre un gruppo elettrogeno che si attiva automaticamente in caso di mancata alimentazione della suddetta cabina.

4.1.3.2. Misure di sicurezza per i PC

Sono attuate misure di sicurezza volte a proteggere i PC dai seguenti rischi:
- accesso fisico non autorizzato.

Per tutelare la riservatezza dei dati contenuti nei PC, sono stabilite le seguenti misure di sicurezza:
- gli accessi ai locali in cui sono dislocate postazioni di lavoro dotate di PC sono presidiati da apposito personale o chiusi a chiave. Negli orari di chiusura al pubblico, in assenza di presidio, gli accessi ai locali sono chiusi a chiave;
- l'accesso ai locali in cui sono dislocate postazioni di lavoro dotate di PC è consentito al personale comunale o equiparato[4]. L'accesso da parte di soggetti esterni all'amministrazione comunale è consentito esclusivamente in presenza di personale comunale e nel rispetto delle regole stabilite per l'accesso del pubblico agli uffici;
- l'accesso alle postazioni di lavoro dotate di PC è consentito esclusivamente a personale comunale o equiparato avente qualifica di designato o autorizzato al trattamento di dati personali o di amministratore di sistema. L'accesso è consentito esclusivamente nei limiti in cui è necessario per lo svolgimento delle mansioni e dei compiti assegnati ai singoli designati o autorizzati, o per lo svolgimento dei compiti di assistenza e manutenzione tecnica assegnati agli amministratori di sistema;
- l'utilizzo dei PC avviene nel rispetto delle seguenti prescrizioni:
  - divieto lasciare le postazioni di lavoro incustodite mentre il PC è acceso e non protetto da salvaschermo[5];
  - obbligo di mantenere la corretta configurazione del PC evitando di alterarne le componenti hardware e software e di installare software non autorizzati;
  - divieto di scaricare sul PC file audio o video o di altro tipo non necessari per lo svolgimento delle mansioni e dei compiti assegnati.

4.1.3.3. Misure di sicurezza per i PC portatili

Sono attuate misure di sicurezza volte a proteggere i PC portatili dai seguenti rischi:
- accesso fisico non autorizzato e furto.

4 lavoratori socialmente utili, lavoratori del “progettone”, lavoratori a progetto, tirocinanti e stagisti, volontari del servizio civile.

5 il salvaschermo si attiva automaticamente dopo 15 minuti di inattività del PC. Lo stesso può inoltre essere attivato cliccando la combinazione di tasti *windows+l*. Lo sblocco del PC avviene cliccando la combinazione di tasti *ctrl+alt+canc* ed inserendo nuovamente la password.

Per tutelare la riservatezza dei dati contenuti nei PC portatili e prevenire il rischio di furto, sono stabilite le seguenti misure di sicurezza:

- i PC portatili, quando non utilizzati, sono custoditi in locali o in elementi di arredo muniti di serratura e chiusi a chiave;
- l'utilizzo dei PC portatili avviene nel rispetto delle seguenti prescrizioni:
  - obbligo di non lasciare il PC portatile incustodito ed accessibile se lo stesso è acceso e non protetto da salvaschermo;
  - obbligo di mantenere la corretta configurazione del PC evitando di alterarne le componenti hardware e software e di installare software non autorizzati;
  - divieto di scaricare sul PC file audio o video o di altro tipo non necessari per lo svolgimento delle mansioni e dei compiti assegnati;
  - divieto di connettere il PC a reti diverse dalla rete informatica comunale, se non strettamente necessario per svolgimento delle mansioni e dei compiti assegnati.

Per tutelare la riservatezza dei dati contenuti nei PC portatili e prevenire il rischio di furto, sono inoltre applicate le seguenti misure tecniche di sicurezza:

- i dischi sono criptati;
- il bios è protetto da password;
- è installato un modulo antivirus aggiuntivo per le connessioni fuori rete aziendale.

4.1.3.4. Misure di sicurezza per i supporti di memorizzazione

Sono attuate misure di sicurezza volte a proteggere i supporti di memorizzazione (hard disk rimovibili, chiavi USB, CD-R/RW, DVD-RW) dai seguenti rischi:

- accesso fisico non autorizzato e furto.

Per tutelare la riservatezza dei dati contenuti nei supporti di memorizzazione e prevenire il rischio di furto, sono stabilite le seguenti misure di sicurezza:

- i supporti di memorizzazione, quando non utilizzati, sono custoditi in locali o in elementi di arredo dotati di serratura e chiusi a chiave;
- prima dell'utilizzo dei supporti di memorizzazione, deve essere eseguita una scansione manuale dell'antivirus;
- i supporti di memorizzazione contenenti dati, se non formattabili per motivi tecnici o se non più utilizzati, sono distrutti;
- i supporti di memorizzazione possono essere riutilizzati esclusivamente previa cancellazione dei dati in essi contenuti[6].

4.1.3.5. Misure di sicurezza per le sale riunioni e le aule corsi

Sono attuate misure di sicurezza volte a proteggere gli strumenti informatici in dotazione delle sale riunioni e delle aule corsi dai seguenti rischi:

- accesso fisico non autorizzato e furto.

6 Per gli hard disk la cancellazione dei dati avviene tramite il comando *FDISK* e la formattazione della partizione successivamente creata. Per gli altri supporti di memorizzazione (hard disk rimovibili, chiavi USB, CD-R/RW, DVD-RW) la cancellazione dei dati avviene tramite l'apposito comando di formattazione.

Per tutelare la riservatezza dei dati contenuti negli strumenti informatici in dotazione delle sale riunioni e delle aule corsi, sono stabilite le seguenti misure di sicurezza:

- le sale riunioni e le aule corsi, quando non utilizzate, sono chiuse a chiave. Le chiavi sono custodite da personale incaricato dal dirigente della struttura comunale competente per la gestione della sala o dell'aula;
- le sale riunioni e le aule corsi sono aperte e chiuse da personale comunale. Non è consentita la consegna delle chiavi a personale esterno all'amministrazione comunale;
- l'utilizzo delle sale riunioni e delle aule corsi avviene alla presenza di personale comunale. L'accesso alle sale e alle aule da parte di personale esterno all'amministrazione comunale è preventivamente autorizzato.

4.2. Misure per il trattamento con ausilio di supporti cartacei

4.2.1. MISURE ORGANIZZATIVE

4.2.1.1. Sistema di autorizzazione

Il sistema di autorizzazione è diretto a disciplinare l'accesso alle banche dati cartacee esistenti nell'organizzazione del Comune di Trento.
I dirigenti designati definiscono i profili di autorizzazione dei singoli autorizzati anteriormente all'inizio del trattamento, in modo da garantire che lo stesso sia svolto esclusivamente con riferimento ai dati necessari per lo svolgimento delle mansioni e dei compiti assegnati.
I dirigenti designati definiscono i profili di autorizzazione con riferimento a singoli autorizzati o a gruppi di autorizzati.
I dirigenti designati definiscono i profili di autorizzazione con riferimento alle seguenti banche dati cartacee:

- fascicoli di protocollo esistenti presso le rispettive strutture;
- eventuali ulteriori banche dati cartacee esistenti presso le rispettive strutture.

I dirigenti designati provvedono con cadenza almeno annuale alla verifica e – se necessario – alla revisione dei profili di autorizzazione dei singoli autorizzati.
La verifica è effettuata sulla base delle seguenti istruzioni:

- Documenti cartacei protocollati
  I documenti cartacei protocollati devono essere trasmessi da ciascun servizio all'Ufficio protocollo e spedizione nel relativo fascicolo a conclusione del singolo procedimento amministrativo. Fino a tale momento l'accesso a tali documenti deve avvenire nel rispetto delle autorizzazioni rilasciate a ciascun dipendente comunale nell'ambito del protocollo informatico PITRE.
  I dirigenti designati procedono alla verifica di tali autorizzazioni sulla base di appositi elenchi resi disponibili distintamente per ciascun servizio comunale ed indicanti i ruoli assegnati a ciascun utente nell'ambito del protocollo informatico PITRE.
- Documenti cartacei non protocollati
  I documenti cartacei non protocollati devono essere eliminati a cura del responsabile del

procedimento a conclusione del singolo procedimento amministrativo. Fino a tale momento l'accesso a tali documenti è consentito esclusivamente al responsabile del procedimento e al personale comunale incaricato della relativa istruttoria. Si precisa che non sono oggetto di eliminazione ma di trasmissione all'Ufficio protocollo e spedizione unitamente al relativo fascicolo i documenti per i quali è previsto uno specifico termine di conservazione dal Piano di conservazione dei documenti cartacei.

4.2.2. MISURE LOGISTICHE E ORGANIZZATIVE

4.2.2.1. Misure di sicurezza per gli archivi e i documenti cartacei

Sono attuate misure di sicurezza volte a proteggere gli archivi e i documenti cartacei dai seguenti rischi:

- accesso fisico non autorizzato.

Per tutelare la riservatezza dei dati contenuti negli archivi e nei documenti cartacei, sono stabilite le seguenti misure di sicurezza:

- i locali in cui sono dislocati archivi cartacei, se situati in posizioni tali da rendere possibili intrusioni, sono muniti di adeguate protezioni, quali l'apposizione di sbarre alle finestre o altre;
- gli accessi ai locali in cui sono dislocati archivi o documenti cartacei sono presidiati da apposito personale. Negli orari di chiusura al pubblico, in assenza di presidio, gli accessi ai locali sono chiusi a chiave;
- l'accesso ai locali in cui sono dislocati archivi o documenti cartacei è consentito al personale comunale o equiparato[7]. L'accesso da parte di soggetti esterni all'amministrazione comunale è consentito esclusivamente in presenza di personale comunale e nel rispetto delle regole stabilite per l'accesso del pubblico agli uffici;
- l'accesso agli archivi e ai documenti cartacei è consentito esclusivamente a personale comunale o equiparato avente qualifica di designato o autorizzato al trattamento di dati personali. L'accesso è consentito esclusivamente nei limiti in cui è necessario per lo svolgimento delle mansioni e dei compiti assegnati ai singoli designati o autorizzati;
- gli archivi e i documenti cartacei sono custoditi in locali o in elementi di arredo muniti di serratura e chiusi a chiave. Le chiavi sono custodite da personale incaricato dal dirigente competente.

4.2.2.2. Misure di sicurezza per i documenti cartacei

Sono attuate misure di sicurezza volte a proteggere i documenti cartacei dai seguenti rischi:

- accesso fisico non autorizzato;
- trattamento illecito di dati personali.

Per tutelare la riservatezza e prevenire trattamenti illeciti dei dati contenuti nei documenti cartacei,

7 lavoratori socialmente utili, lavoratori del "progettone", lavoratori a progetto, tirocinanti e stagisti, volontari del servizio civile

sono stabilite le seguenti misure di sicurezza:

- la consultazione dei documenti cartacei è consentita esclusivamente a personale comunale o equiparato avente qualifica di designato o autorizzato al trattamento di dati personali. La consultazione è consentita esclusivamente nei limiti in cui è necessaria per lo svolgimento delle mansioni e dei compiti assegnati ai singoli designati o autorizzati;
- la consultazione dei documenti cartacei è consentita per il tempo strettamente necessario allo svolgimento delle mansioni e dei compiti assegnati ai singoli designati o autorizzati. Una volta espletati tali mansioni e tali compiti, i documenti sono riposti nei locali o negli elementi di arredo in cui sono custoditi;
- i documenti cartacei non sono lasciati incustoditi. In tutti i casi di allontanamento dei designati o degli autorizzati dalle postazioni di lavoro, i documenti sono riposti nei locali o negli elementi di arredo in cui sono custoditi;
- i documenti cartacei contenenti dati particolari o giudiziari sono custoditi separatamente dagli altri documenti, in busta chiusa all'interno dei fascicoli.

ELENCO ALLEGATI

NUMERO	DESCRIZIONE
2.2.A	Modelli di clausole in materia di trattamento di dati personali (da inserire in bandi/disciplinari/capitolati/contratti)
2.2.B	Schema di atto di nomina di responsabili del trattamento di dati personali (da allegare a bandi/disciplinari/capitolati)
2.2.C	Modello di nomina di autorizzati al trattamento dati personali (soggetti interni all'amministrazione comunale)
2.2.D	Modello di nomina di autorizzati al trattamento dati personali (soggetti esterni all'amministrazione comunale)
2.2.E	Modello di nomina di referenti informatici
3.1.A	Check list verifica adempimenti privacy
3.1.B	Modello di informativa/liberatoria per la pubblicazione di video e immagini
3.2.A	Modello di informativa sul trattamento di dati personali
3.3.A	Elenco dei dipendenti comunali individuati quali referenti per l'implementazione del registro delle attività di trattamento di dati personali
3.3.B	Istruzioni per l'implementazione del registro delle attività di trattamento di dati personali
3.3.C	Istruzioni per l'utilizzo dell'applicativo contenente il registro delle attività di trattamento di dati personali