COMUNE DI CERVASCA

Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali-

MODELLO ORGANIZZATIVO

1. Finalità e ambito d'applicazione

1.1 Finalità

Il presente regolamento rappresenta il Modello Organizzativo Privacy (MOP) ed ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Cervasca.

Con l'osservanza di questo modello s'intende richiamare tutte le risorse operanti all'interno del Comune di Cervasca al rispetto della normativa sulla sicurezza dei dati personali, con espressa attenzione all'impiego delle risorse informatiche.

Deve essere aggiornato in relazione alla evoluzione del settore; la redazione e l'aggiornamento deve essere approvato con delibera comunale.

Nel caso in cui subentrino nel corso dell'anno modifiche che implichino ulteriori revisioni del MOP, queste devono essere predisposte in tempi rapidi e senza indebiti ritardi.

Le modalità di approvazione, gestione e diffusione del MOP sono sotto la responsabilità del Titolare del trattamento. La valutazione degli aspetti informatici è stata svolta dall'Amministratore del sistema.

1.2 Ambito d'applicazione delle presenti direttive

Questo manuale è vincolante per il personale del Comune di Cervasca, sia dipendente sia collaboratore.

1.3 Modifiche rispetto alla edizione precedente

Il MOP è alla prima emissione. Il Comune di Cervasca ha deciso di tenere sotto controllo, tramite l'aggiornamento del MOP medesimo, gli aspetti relativi all'applicazione del Regolamento Europeo Privacy, a maggiore garanzia delle attività svolte e dei controlli effettuati.

1.4 Riferimenti normativi e documentali

Regolamento Europeo Ue n. 679/2016 sulla protezione dei dati personali, i pareri de Garanti europei Wp 29 e i provvedimenti del Garante.

1.5 Pianificazione degli interventi previsti per il prossimo periodo

Il presente documento è integrato con le misure minime di sicurezza agli atti che riportano in modo analitico le implementazioni necessarie al fine di adeguare l'infrastruttura almeno allo "standard minimo" previsto dalla AGID. Le future relazioni di evoluzione ed implementazione costituiranno automatica modifica al presente regolamento.

2. Trattamenti di dati personali

2.1 Finalità del trattamento

I trattamenti sono compiuti dal Comune per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

✓ l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;

✓ la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;

✓ l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

c) l'esecuzione di un contratto con soggetti interessati;

d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

2.2 Elenco dei trattamenti nell'ambito di attività del Comune

Nell'ambito della propria attività, il Comune di Cervasca tratta dati personali e dati particolari, al fine di adempiere ai propri obblighi tipici di un Ente Pubblico, con particolare riferimento ai compiti che la legge attribuisce agli Enti Locali.

Il Comune di Cervasca pone quindi la massima attenzione a che i dati siano trattati in modo lecito, corretto e sicuro, al fine di ridurre al minimo il rischio che i dati vadano distrutti o persi, anche a causa di eventi accidentali, e che persone non autorizzate li possano leggere, modificare, o utilizzare in modo improprio o diverso dallo scopo per cui sono stati raccolti.
A tal fine è stato predisposto il Registro dei trattamenti.

2.3 Titolare del trattamento

Il Titolare del trattamento nella persona del legale rappresentante del Comune:
✓ è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
✓ mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
✓ Attua gli interventi necessari per la realizzazione delle misure nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
✓ adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

✓ Effettua nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la

natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

- ✓ inoltre, provvede a:
  a) nominare il Responsabile della protezione dei dati;
  b) nominare quali Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;
  c) predisporre l'elenco degli autorizzati del trattamento dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente (in relazione alle dimensioni organizzative del Comune);
- ✓ nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

2.4 Data Protection Officer

Il Titolare individuerà con proprio provvedimento la risorsa esterna dotata di adeguata esperienza, capacità ed affidabilità per assumere il ruolo di Responsabile DPO. La funzione riceve autorità dall'Organo di Governo e la sua nomina è prevista per obbligo legislativo.

I principali compiti del DPO nei confronti del Comune di Cervasca, in relazione agli aspetti relativi all'applicazione del Regolamento Privacy sono:

- verificare l'attuazione e l'applicazione del Regolamento sia una volta ultimato l'adeguamento da parte dell'ente sia a fronte di aggiornamenti normativi e/o giurisprudenziali

- informare e consigliare il titolare del trattamento, nonché lo staff dirigenziale e/o i dipendenti in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- tenere i rapporti con il Garante ed effettuare le notifiche e le comunicazioni previste dalla legge.
- Fornire se richiesto un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e tutti gli adempimenti conseguenti.

La funzione fornisce al Titolare del trattamento elementi di valutazione sull'applicazione della norma (valutazione del rischio, registro per il trattamento dei dati personali, valutazioni di impatto del rischio) contribuendo all'adeguamento delle disposizioni, in relazione agli aggiornamenti di legge.

Il DPO inoltre deve:

- partecipare a riunioni ogni qualvolta si introduca all'interno dell'ente una nuova tecnologia o debbano essere attuate compagne o operazioni che riguardino il trattamento dei dati personali e impostare unitamente al Titolare del trattamento la valutazione preventiva di impatto del rischio;
- partecipare a riunioni ogni qualvolta si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche dell'ente che impattano sulla riservatezza dei dipendenti;
- fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
- redigere risposte ad hoc in caso di esercizio da parte dell'interessato dei diritti previsti a suo favore e conseguente comunicazione agli altri eventuali titolari del trattamento.

La funzione deve operare in accordo a quanto previsto nella lettera di nomina ed è membro del Team di crisi in caso di Data Breach in collaborazione con gli autorizzati al trattamento.

2.5 Autorizzati al trattamento

Gli autorizzati al trattamento sono designati, singolarmente, dal Titolare del trattamento per le relative banche dati. Le responsabilità sono dettagliate per iscritto nella lettera di

nomina o in altri documenti. Tra gli autorizzati si identificano figure apicali e subordinate.
L'elenco delle banche dati allegato ai provvedimenti di nomina registra la situazione allo stato attuale e viene aggiornato annualmente.

2.6 Responsabili esterni

L'affidamento all'esterno (outsourcing) di parti di attività di trattamento dati relativi al Comune di Cervasca comporterà l'obbligo, identificato specificatamente all'interno del contratto di servizio o di elaborazione, da parte del terzo di applicazione dell'intera normativa sulla privacy, sia, a puro titolo esemplificativo in relazione alle modalità di trattamento e comunicazione dei dati, sia soprattutto in relazione alle Misure di Sicurezza.
Tutti i soggetti esterni, sottoscrivono un accordo con il Comune che disciplina esattamente gli ambiti di responsabilità e di obblighi che le parti sono tenute ad assumere e che si impegnano ad effettuare. Tutte le Ditte ed i soggetti che operano attraverso propri dipendenti e collaboratori si obbligano a rendere edotti queste persone di tutto quanto previsto dagli accordi ed in generale dalla normativa sulla privacy.
Tali società sono formalmente impegnate ad operare nel rispetto della normativa vigente e a garantire la segretezza delle informazioni riservate a cui dovessero accedere nell'esecuzione del proprio lavoro, nonché ad attestare per iscritto la conformità degli interventi effettuati sul sistema. L'elenco dei responsabili esterni viene aggiornato annualmente. Essi possono essere chiamati a far parte del Team di crisi in caso di Data Breach.

2.8 Amministratore di sistema

Per quanto concerne la funzione dell'Amministratore di sistema, la nomina è esterna.
La funzione è delegata dal Titolare del trattamento ad accedere al server di rete tramite la password di sistema e accedere ai dati di un utente assente, in caso di oggettive necessità di lavoro e sicurezza, in conformità alla procedura esplicitata al punto 4.2.
L'Amministratore di Sistema supporta il Titolare del trattamento dei dati personali nella valutazione dell'attuale sistema informatico in una prospettiva di sviluppo, contribuendo alla scelta di soluzioni (acquisti o modifiche al sistema) che, valutando da una parte le esigenze fondate del personale e dall'altra le possibilità tecniche di hardware e software offerte dal mercato, diano priorità al rapporto costi e profitti e possano al

contempo assicurare l'impiego efficiente dell'informatica all'interno del Comune di Cervasca. I principali compiti del ADS nei confronti del Comune di Cervasca, in relazione agli aspetti relativi all'applicazione del Regolamento Privacy sono dettagliati per iscritto nella lettera di nomina o in altri documenti. Esso è membro del Team di crisi in caso di Data Breach.

3. Analisi dei rischi

3.1 Sicurezza del Trattamento

Il Comune di Cervasca e ciascun Responsabile/ Autorizzato del trattamento mettono in atto a fronte dei pericoli individuati misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

3.1.1 Fonti di pericolo

Buona parte dei danni può insorgere da parte sia di collaboratori dell'azienda sia di terzi:

- involontariamente (errori di manipolazione);
- per negligenza (inavvertenza, leggerezza);
- in mala fede (atto criminale).

I rischi possono essere causati da:

- Comportamenti degli operatori
  - Furto di credenziali di autenticazione
  - Carenza di consapevolezza, disattenzione o incuria
  - Comportamenti sleali o fraudolenti
  - Errore materiale
- Eventi relativi agli strumenti
  - Azione di virus informatici o di codici malefici
  - Spam o altre tecniche di sabotaggio
  - Malfunzionamento, indisponibilità o degrado degli strumenti
  - Accessi esterni non autorizzati
  - Intercettazione di informazioni in rete

- Eventi relativi al contesto

  Accessi non autorizzati a locali/reparti ad accesso ristretto

  Asportazione e furto di strumenti contenenti dati

  Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria

  Guasto ai sistemi complementari (impianto elettrico, climatizzazione….)

  Errori umani nella gestione della sicurezza fisica.

3.1.2 Misure tecniche ed organizzative

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile/Autorizzato del trattamento:

✓ sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);

✓ misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

Il Comune di Cervasca e ciascun Responsabile/Autorizzato del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

I nominativi ed i dati di contatto del Titolare, del o dei Responsabili/Autorizzati del trattamento e del Responsabile della protezione dati sono pubblicati sul sito

istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.
L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

3.1.3 Analisi del rischio

E' stata effettuata l'analisi dei rischi, per la compilazione della quale è stata utilizzata l'istruzione analisi del rischio Dall'analisi dei rischi sono emersi:

✓ misure di mitigazione da mettere in atto nel prossimo periodo che vanno ad integrare quelle dell'allegato AGDS;
✓ l'individuazione dei trattamenti per i quali è prevista l'effettuazione della DPIA.

3.2 Valutazione Impatto

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, RGDP.

La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono indicati nella linea guida WP 148 del 04.10.2017 concernenti la valutazione d'impatto, i seguenti:

1) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

2) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

3) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

4) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;

5) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione

di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

6) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

7) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

8) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

9) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare

un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

L'RPD deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

L'ADS, ed eventualmente l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

L'Amministratore del sistema, può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

La DPIA non è necessaria nei casi seguenti:

- ✓ se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;
- ✓ se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- ✓ se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- ✓ se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

La DPIA è condotta prima di dar luogo al trattamento, attraverso un documento che contiene le seguenti informazioni:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

3.3 Approfondimenti

3.3.1 Aspetti legali

Solo i software di cui si disponga della licenza sono validi. Questo principio fa parte delle direttive quadro del Comune di Cervasca. La violazione di questo principio rappresenta un reato punibile penalmente. Allo stesso modo, è di regola punibile la contemporanea installazione di una licenza su più sistemi. Una licenza valida costituisce in ogni caso il presupposto per il supporto da parte del produttore o commerciante.

4 Misure tecniche di protezione e ripristino della disponibilità dei dati

Le seguenti misure di sicurezza contribuiscono in maniera essenziale alla sicurezza dell'ambiente informatico. Esse devono essere sistematicamente messe in atto,

rispettate e controllate da ogni collaboratore Gli autorizzati al trattamento sono infatti tenuti ad attenersi alle sue prescrizioni.

Sono applicati due tipi di misure di sicurezza:

- Prevenzione dei danni, ossia misure preventive (che hanno la massima priorità);
- Diminuzione dei danni: misure atte a mantenere la conseguenza del danno la più ridotta possibile.

4.1.1 Interventi sul sistema informatico

Gli interventi sul sistema informatico sono effettuati dall'ADS la quale al termine di ogni intervento rilascia un rapporto di intervento.

4.2 Misure generali in capo all'ADS

Le misure generali applicate nel Comune di Cervasca sono volte alla protezione ed al ripristino della disponibilità dei dati sono le seguenti dettagliate nella lettera di nomina dell'ADS.

4.3 Livello di sicurezza dei server e password di accesso

Le misure generali applicate nel comune di Cervasca sono volte alla protezione e al ripristino della disponibilità dei dati sono dettagliate nell'incarico dell' ADS.

4.3.1 Password di accesso ai server

La password di accesso ai server, ai back-up ed al server sono specificate nelle disposizioni di sicurezza descritte nelle misure minime di sicurezza.

Le parole chiave di qualunque tipo devono rispettare le indicazioni contenute nel Regolamento Comunale.

4.3.2 Protezione da virus

L'utilizzo di supporti di dati esterni (dischetti, memorie USB), allegati di e-mail e file trasferiti richiede cautela. Anche l'acquisizione di informazioni da Internet comporta il pericolo di infettarsi con virus.

Pertanto è necessario richiamare l'attenzione di ogni utente sulla sua responsabilità rispettando le le indicazioni contenute nel Regolamento Comunale.

4.4 Sistemi di Back-up, schema di rete e cablaggi

Le disposizioni di sicurezza sono descritte dell'Allegato C "Direttiva AGID "Misure Minime di Sicurezza ICT nella P.A."

4.5 Sicurezza server

Le disposizioni di sicurezza sono descritte dell'Allegato C "Direttiva AGID "Misure Minime di Sicurezza ICT nella P.A."

4.6 Misure edilizie

Gli accessi alle parti comuni dell'edificio devono essere chiusi (a chiave nel caso delle porte) negli orari in cui il Comune è chiuso al pubblico. Negli orari di apertura al pubblico, nessun dato personale deve essere posto in vista, o deve essere facilmente accessibile o riconoscibile a chiunque.

Si richiamano inoltre le disposizioni già segnalate nel paragrafo relativo all'Analisi dei Rischi. Vediamo ora le disposizioni riguardanti specifici locali:

- **Uffici**

L'accesso agli Uffici è strettamente controllato da parte degli Autorizzati al trattamento che effettuano trattamenti di dati personali. Durante il normale orario di apertura degli Uffici, l'accesso ai dati è controllato dai rispettivi autorizzati al trattamento e qualora, per motivi diversi, un Ufficio rimanga temporaneamente vuoto, l'autorizzato al trattamento è obbligato a chiudere a chiave la porta d'accesso dello stesso e custodire la copia di chiavi che ne permettono l'apertura (ovvero consegnarla al collega o ad altro soggetto che comunque abbia diritto ad espletare la propria attività nel medesimo Ufficio).

In ogni caso, ciascun autorizzato al trattamento deve rendere i dati personali specificamente trattati non consultabili o visibili da parte di eventuali terzi che abbiano diritto ad accedere all'Ufficio né al collega che stia svolgendo il proprio lavoro nel medesimo locale. I terzi che possono accedere agli Uffici negli orari di apertura e/o di chiusura sono espressamente determinati in apposite autorizzazioni loro conferite, nelle quali sono indicate le responsabilità loro riferite, quale ad esempio il personale di pulizia.

Tutti gli autorizzati al trattamento devono provvedere a non lasciare mai, in loro assenza, porte e finestre dei rispettivi Uffici aperte. Gli accessi specifici (cassetti,

armadi, ecc.) vanno chiusi a chiave sempre, le porte solo in assenza degli addetti dai rispettivi Uffici. Tutti i dati sensibili contenuti su documenti cartacei devono sempre essere conservati dentro armadi o contenitori chiusi a chiave.

- **Locali archivio**

Gli archivi storici e correnti degli atti comunali devono essere chiusi a chiave ed i dati conservati devono essere riposti in modo organizzato e sistematico, salvo che non rivestano più alcuna utilità per l'attività ordinaria di trattamento.

- **Sicurezza archivi cartacei**

Si ritiene fondamentale evidenziare le istruzioni al trattamento riguardanti la complessiva attività del Comune, la cui applicazione pratica risulta essere di vitale importanza per la concreta applicazione del presente Modello Organizzativo. In particolare tutte le informazioni riportate su documenti cartacei, delle quali si abbia effettiva esigenza di consultazione, devono essere prelevate e detenute in base alla loro attinenza e pertinenza con il trattamento richiesto.

Gli archivi sono ad accesso selezionato, cioè è possibile ricercare ed estrarre esclusivamente i dati necessari per il trattamento. Se si tratta di dati particolari o relativi a condanne penali e reati, ai sensi degli art. 9 e 10 del GDPR 679/2016, gli autorizzati al trattamento devono utilizzare esclusivamente i dati strettamente necessari allo svolgimento delle proprie mansioni ed immediatamente restituirli al termine delle operazioni.

I dati particolari o relativi a condanne penali e reati, così come sopra definiti, devono essere conservati dentro contenitori muniti di serratura. Se una o più informazioni devono rimanere a disposizione per un trattamento prolungato o continuo, l'incaricato deve essere sempre presente nel locale ove avviene il trattamento ed essere in grado di impedire a terzi di vedere la documentazione in uso. Nel caso in cui sia indispensabile l'accesso al locale da parte di terzi, l'autorizzato al trattamento provvede preventivamente a riporre tutti i dati personali in consultazione nei relativi siti protetti.

Tutti i soggetti, interni o esterni all'ente, che possono accedere all'edificio o anche ai dati cartacei sono muniti di esplicita autorizzazione, recante in dettaglio le regole per il corretto trattamento dei dati e/o i limiti e le responsabilità connesse al loro diritto di accesso. Tali autorizzazioni sono periodicamente controllate, al fine di verificare la loro osservanza ed adeguatezza alle condizioni di espletamento dei servizi ed in relazione

alle motivazioni per le quali sono state assegnate.

Il dipendente/collaboratore ha l'obbligo di:

- evitare che persone non autorizzate possano leggere, copiare o comunque impossessarsi dei dati personali in sua custodia
- restituire o distruggere gli atti e i documenti contenenti dati personali al termine delle operazioni affidategli.

Il contenuto degli armadi è accessibile al solo collaboratore/dipendente.

Gli armadi devono essere chiusi quando il dipendente/collaboratore abbandona il proprio ufficio**.**

- **Archivio documenti dei dipendenti**

I documenti dei dipendenti, contenenti dati sensibili e personali, sono archiviati in armadi chiusi gestiti dall'ufficio personale che li tratta.
All'atto dell'assunzione ad ogni dipendente viene data l'informativa.I certificati di Malattia vengono comunicati direttamente tramite il portale INPS con il codice assegnato dal medico Curante.
Gli altri documenti sono trattati dall'ufficio personale e trasmessi alla società che elabora gli stipendi quanto necessario. Anche in questo caso i documenti sono archiviati nella cartella del dipendente.

- **Archivio del casellario giudiziario**

I documenti sono conservati dagli uffici che li hanno richiesti in armadi chiusi a chiave.

4.7. Applicazione normativa D.lgs 81/2008

Il Comune di Cervasca applica la normativa sulla sicurezza dei luoghi di lavoro e la normativa sul fumo.

Sono attivi gli estintori, soggetti a manutenzione semestrale.

Tutto il personale è regolarmente aggiornato a cura del Responsabile della sicurezza ai sensi di legge.

4.7.1 Videosorveglianza

Nel Comune di Cervasca è attivo un sistema di videosorveglianza.

Gli scopi dell'attività di video sorveglianza rispondono alle funzioni istituzionali demandate agli Enti Locali dalle norme nazionali, dall'ordinamento della Polizia Municipale, o dagli statuti e dai regolamenti comunali, quali la sicurezza pubblica e la prevenzione o l'accertamento dei reati. Il regolamento Comunale per l'installazione e l'utilizzo degli impianti di videosorveglianza e delle fototrappole ha ricevuto il vaglio della Commissione Prefettizia.
I cittadini sono informati della presenza di telecamere e dei diritti che possono esercitare sui propri dati.

L'interessato ha diritto di opporsi, in tutto o in parte:

- per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

L'uso di tali dati personali non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali. L'informativa al cittadino ha luogo nei punti e nelle aree in cui si svolge la video sorveglianza.
I dati raccolti sono quelli strettamente necessari agli scopi perseguiti, classificabili in:

- sistemi di rilevazione e controllo dei flussi di traffico;
- sistemi di rilevazione delle infrazioni al codice della strada;
- sistemi di vigilanza del pubblico trasporto;
- sistemi di controllo dei perimetri e degli spazi di stabilimenti ed edifici pubblici da sottoporre a particolare tutela;
- sistemi di controllo della aree di raccolta dei rifiuti.
- parcheggi e aree pubbliche a rischio.

e sono pertanto solo registrate le immagini indispensabili, limitando l'angolo visuale della ripresa, evitando immagini dettagliate o ingrandite e stabilendo in maniera adeguata la localizzazione delle telecamere e modalità di ripresa.
La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in

relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.
Solo in alcuni specifici casi è ammesso un tempo più ampio di conservazione dei dati, che non può comunque superare la settimana.
Un eventuale allungamento dei tempi di conservazione è valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.
Il cittadino potrà rivolgersi per esercitare il diritti di rettifica, aggiornamento o cancellazione delle informazioni che lo riguardano al Responsabile dei servizi di polizia municipale.

Sono state individuate, con designazione scritta, le persone che possono utilizzare gli impianti e prendere visione delle registrazioni ed è vietato l'accesso alle immagini ad altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia.
L' autorizzato del trattamento per gli impianti di videosorveglianza è designato, dal Titolare del trattamento, avendo in carico le responsabilità dettagliate per iscritto nella lettera di nomina (allegato 3) o in altri documenti.
La nomina è conservata presso l'ufficio Referente Privacy.

4.7.2 Posta elettronica e accesso da remoto alla posta elettronica

Al momento, nessun operatore ha le credenziali per collegarsi alla posta elettronica in remoto.

5 Misure organizzative di protezione e ripristino della disponibilità dei dati

5. 1 Regolamento comunale:

Per tutti i dipendenti/collaboratori che hanno accesso a dati personali o ne eseguono l'elaborazione valgono le disposizioni contenute nel Regolamento Europeo 679/2016 in materia di protezione dei dati personali.

Per impedire che il personale entri inutilmente in conflitto con le disposizioni della legge, il Comune di Cervasca sottoscrive con i propri dipendenti e collaboratori operanti in sede il Regolamento comunale, che disciplina le disposizioni in merito all'accesso e all'impiego dei mezzi informatici.

Il medesimo regolamento deve essere sottoscritto da chiunque abbia accesso autorizzato al sistema informatico, anche temporaneo (ad esempio collaboratori occasionali, stagisti …), in qualità di “autorizzato al trattamento”.

5.2 Formazione iniziale e continua

Gli autorizzati per il trattamento dei dati interni del Comune sono individuati tra risorse dotate di adeguata esperienza, capacità ed affidabilità in base alle esigenze di trattamento dei dati presenti nella organizzazione.

Il Titolare del trattamento è responsabile della formazione del personale incaricato del trattamento dei dati al fine di renderlo consapevole:

- dei rischi che incombono sui dati
- delle misure per prevenire eventi dannosi
- della disciplina sulla protezione dei dati più rilevanti in rapporto alle rispettive attività
- delle responsabilità che ne derivano
- delle modalità per aggiornarsi sulle misure minime adottate dal Comune

Tale formazione avviene con frequenza e in occasione di cambiamenti di mansioni e dell’introduzione di nuovi e significativi strumenti rilevanti per il trattamento dei dati.

Il Titolare del trattamento completa inoltre la formazione del personale relativamente alle modalità di gestione del sistema informatico e, se necessario, del software applicativo, in base al livello di competenza delle risorse. Laddove opportuno, il DPO collabora alla ricerca di offerenti di corsi e relatori esterni.

5.2.1 Formazione iniziale

Il Titolare del trattamento prevede per ogni nuova risorsa da inserire in organico un modulo dedicato al tema della protezione dei dati personali all’interno del programma di formazione iniziale, con consegna e illustrazione delle indicazioni in merito all’applicazione del Regolamento Europeo 679/2016; ciò avviene, in particolare con la consegna della nomina come incaricato.

Deve inoltre essere effettuata, se necessario, un’azione formativa sulle modalità di gestione del sistema informatico e, se necessario in base alla valutazione iniziale delle competenze informatiche della nuova risorsa, un’ulteriore azione formativa relativa al software applicato.

5.2.2 Formazione continua

Il Comune di Cervasca, ritiene di primaria importanza il tema della Protezione dei dati personali, per tutte le risorse in organico per l'anno 2018.

Per gli anni successivi, in occasione degli aggiornamenti annuali del MOP, il DPO, nel rendere noto il nuovo testo, organizzerà, se necessario ed in relazione alla rilevanza delle variazioni intervenute, attività formative per segnalare le modifiche e innovazioni intervenute in materia di protezione dei dati personali e di gestione del sistema informatico. Ulteriore formazione, in materia di privacy, verrà pianificata ed eseguita a seguito dell'introduzione del Regolamento Europeo sul trattamento dei dati.

Nel caso dovessero intervenire nel corso dell'anno modifiche o innovazioni tali da necessitare un aggiornamento urgente di tutte le risorse il DPO provvederà alla organizzazione delle attività formative secondo le esigenze.

5.3 Procedura di dimissione

Nel caso di dimissione di un collaboratore il Titolare

- archivia la documentazione del collaboratore;
- comunica all'ADS le dimissioni del collaboratore affinché, quest'ultimo possa provvedere a: disattivare la connessione da remoto del collaboratore, reindirizzare la posta elettronica, recuperare la postazione;
- comunica all'ufficio personale la dimissione del collaboratore, affinché, possa provvedere al ritiro degli strumenti di ausilio alla attività (cellulare, chiavi, ecc.)

La procedura di dismissione di un account prevede, data la necessità di mantenere l'indirizzo attivo per la ricezione di eventuali mail, la seguente prassi: nel giorno in cui l'autorizzato al trattamento, cessa il suo rapporto di collaborazione con il Comune, la password del suo account viene modificata dall'Amministratore di Sistema, inoltre viene implementata una regola di risposta automatica e un redirect della posta ad un altro account individuato sulla base della tipologia di attività svolta da collaboratore non più presente.

Successivamente, l'account viene definitivamente cancellato unitamente a tutte le mail che contiene, da parte dell'Amministratore di Sistema.

6 Informativa e consenso

6.1 Informativa per utenti dei servizi comunali

Ai cittadini viene comunica l'informativa per il trattamento dei dati. Qualunque uso non previsto dai fini istituzionali di utilizzo di dati di cittadini, deve essere autorizzato dalla Titolare del trattamento dei dati o dal DPO e deve essere attuato nel rispetto della normativa di legge.

6.2 Informative dipendenti

Ai dipendenti viene comunica l'informativa per il trattamento dei dati.

Tali dati personali, ai sensi dell'art 6 lett b) del Regolamento europeo n. 16/679, possono essere trattati senza il suo consenso in quanto necessari all'esecuzione del contratto.

Qualunque uso non previsto dall'esecuzione del contratto dei dati dei dipendenti, deve essere autorizzato dal Titolare del trattamento dei dati o dal DPO e deve essere attuato nel rispetto della normativa di legge.

6.3 Informativa per referenti di fornitori

Sono dati di persona giuridica di cui si possiedono dei dati personali (es. nome e contati del referente); a tali soggetti, essendo una Pubblica Amministrazione, non è prevista la raccolta del consenso, ma solo della informativa. Quest'ultima è disponibile sul sito internet del Comune.

7 Data Breach

Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.

Il Responsabile/Autorizzato del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Il Team del Data Breach è composto dal Titolare dall' RDO, dal Segretario Comunale dai Responsabili di P.O e dall'Amministratore del sistema se ritenuto necessario.

7 Norme finali

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le norme del RGDP e tutte quelle attualmente ancora vigenti.

Terminologia

1. Terminologia afferente al Regolamento Europeo 679/2016

Banca di dati:

> "qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti"

Comunicazione:

> "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, del responsabile e degli autorizzati al trattamento, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"

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".

Dato/i Personale/i" "Categorie Particolari di Dati"

> "ogni Dato Personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (anche detti "Dati Sensibili" ai sensi del D.lgs. 196/2003)".

Dati giudiziari:

> "ogni Dato Personale relativo a condanne penali e ai reati o a connesse misure di sicurezza ovvero relativo a provvedimenti giudiziari, sanzioni penali, o carichi pendenti, o la qualità dell'imputato o indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale".

Diffusione:

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

Autorizzati al trattamento:

"le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile e che agiscono sotto l'autorità del Titolare o del Responsabile ai sensi dell'art. 30 del Codice Privacy e dell'art. 29 del GDPR".

Interessato:

"la persona fisica, la persona giuridica, l'ente o l'associazione a cui si riferiscono i dati personali"

Responsabile:

"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che tratta dati per conto del Titolare del trattamento dei Dati Personali".

Titolare:

"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Ai fini del presente atto con il termine Titolare si intende il Comune di _____".

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".

2. Terminologia afferente al sistema informatico

Cookie:

I cookie consentono al Web Master di perfezionare l'offerta e al visitatore di interagire più rapidamente. ciononostante, i cookie godono di cattiva fama. Un cookie può ad esempio essere del tipo seguente:

www.ora.com FALSE I FALSE 946684799 ora-account 123

I cookie sono informazioni testuali, che vengono depositate in un file speciale sul disco rigido la workstation. I cookie non possono contenere alcun virus. Vi sono contenute le informazioni, di cui il Web Server ha bisogno per potervi servire meglio. I file dei cookie sono raramente di grandezza superiore a 3000 bytes e i cookie risalenti a più di 30 giorni vengono di regola cancellati automaticamente.

Esempio:

Se si inizia una ricerca presso uno dei grandi motori di ricerca, insieme al risultato arriva un cookie contenente le seguenti informazioni:

- Cosa è stato cercato
- Cosa è stato trovato
- Come si può proseguire la ricerca

Dominio:

Un nome o un indirizzo per minimo un computer o un intero gruppo di computer raggruppati dal punto di vista geografico, organizzativo o tematico (ad es. tutti i computer dell'XXX SRL costituiscono il dominio www.XXX SRL.it)

E-Mail:

Abbreviazione per Electronic Mail (posta elettronica). Mediazione di messaggi e corrispondenza tramite reti di comunicazione disponibili in tutto il mondo.

Internet:

Rete mondiale di computer, strutturata in modo non gerarchico. È composta di diversi servizi, operanti secondo standard unificati. I servizi più noti sono E-Mail, FTP e WWW.

Intranet:

Rete chiusa di aziende o gruppi di aziende, che fa uso delle tecnologie di Internet.

Extranet:

Una intranet, in cui sono collegati i clienti, i fornitori e i partner, che comunicano tramite Internet utilizzando nomi utente e password predefiniti. L'intranet viene per così dire estesa in Internet, costituendo tutta via un'area protetta.