

COMUNE DI CERMENATE

Regolamento sulla protezione dei dati personali adottato in attuazione del Regolamento (UE) 2016/679

SOMMARIO

INTRODUZIONE

CAPO I – DISPOSIZIONI GENERALI

Art. 1 Definizioni

Art. 2 Quadro normativo di riferimento

Art. 3 Oggetto

Art. 4 Finalità

CAPO II – PRINCIPI

Art. 5 Principi e responsabilizzazione

Art. 6 Liceità del trattamento

Art. 7 Condizioni per il consenso

Art. 8 Informativa

Art. 9 Sensibilizzazione e formazione

CAPO III – IL TRATTAMENTO DEI DATI PERSONALI

Art. 10 Trattamento dei dati personali, ricognizione dei trattamenti e indice dei trattamenti

Art.11 Tipologie di dati trattati

Art. 12 Trattamento dei dati particolari e giudiziari

Art.13 Trattamento dei dati particolari all'interno del Comune

Art. 14 Trattamento dei dati del personale

Art. 15 Rilevanza delle schede/tabelle identificative delle tipologie di tipi di dati particolari e giudiziari per cui è consentito il relativo trattamento

Art. 16 Registro delle attività di trattamento e delle categorie di trattamento

CAPO IV – DIRITTI DEGLI INTERESSATI

Art. 17 Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

Art. 18 Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

Art. 19 Diritti dell'interessato

Art. 20 Diritto di accesso

Art. 21 Diritto alla rettifica e cancellazione

Art. 22 Diritto alla limitazione

Art. 23 Diritto alla portabilità

Art. 24 Diritto di opposizione e processo decisionale automatizzato relativo alle persone

Art. 25 Modalità di esercizio dei diritti dell'interessato Art. 26 Indagini difensive

CAPO V – SOGGETTI

Art. 27 Titolare e contitolari

Art. 28 Dirigenti e Responsabili di Posizione organizzativa-P.O.

Art. 29 Responsabili del trattamento e sub responsabili

Art. 30 Incaricati esterni del trattamento

Art. 31 Incaricati del trattamento non dipendenti del titolare

Art. 32 Amministratore di sistema

Art. 33 Responsabile della protezione dei dati personali (RPD) – Data Protection Officer (DPO)

CAPO VI – SICUREZZA DEI DATI PERSONALI

Art. 34 Misure di sicurezza

Art. 35 Valutazione d'impatto sulla protezione dei dati/DPIA

Art. 36 Pubblicazione sintesi della valutazione d'impatto – DPIA

Art. 37 Consultazione preventiva

Art. 38 Modulistica e procedure

Art. 39 Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

Art. 40 Notificazione di una violazione dei dati personali

Art. 41 Comunicazione di una violazione dei dati personali

Art. 42 Disposizioni finali

INTRODUZIONE

Il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, con abrogazione della direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

Il nuovo regolamento UE, che si applica negli Stati membri a decorrere dal 25 maggio 2018, si fonda sulla affermazione che la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale come risulta anche dalla circostanza che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Per rafforzare la protezione, il Regolamento UE, introduce numerose e rilevanti novità partendo da un approccio, fondato sul principio di cautela, basato sul rischio del trattamento e su misure di accountability di titolari e responsabili (come la valutazione di impatto, il registro dei trattamenti, le misure di sicurezza, la nomina di un RDP-DPO).

Come ha evidenziato il Garante nella guida all'applicazione del Regolamento, la nuova disciplina europea pone con forza l'accento sulla "responsabilizzazione" (accountability) di titolari e responsabili ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Tra i criteri che i titolari e i responsabili sono tenuti ad utilizzare nella gestione degli obblighi vi sono:

- il criterio del "data protection by default and by design", ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati;

- il criterio del rischio inerente al trattamento, da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati, impatti che devono essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.

Ne consegue che l'intervento delle autorità di controllo, nel nuovo impianto gestionale, è destinato a svolgersi principalmente ex post, ossia a collocarsi successivamente alle determinazioni assunte autonomamente dal Titolare; ciò spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del Titolare/Responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di

adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

Il diritto alla privacy è un diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità. Per questi motivi la cultura della privacy necessita di crescere e rafforzarsi, principalmente fra gli operatori delle pubbliche amministrazioni, perché solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di legge, nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza. Il Titolare intende adeguare e conformare la propria normativa regolamentare alle novità introdotte dal citato regolamento UE, fermo restando che il presente aggiornamento è destinato ad essere ulteriormente revisionato in presenza di sopravvenienza di linee guida del Garante per protezione dei dati personali, o di novità normative e giurisprudenziali.

L'adeguamento al Regolamento UE lascia impregiudicate le disposizioni contenute nel D.Lgs. 30 giugno 2003, n. 196 (Codice privacy) nella parte non incompatibile con il nuovo regolamento europeo, le quali disposizioni, anche dopo il 25 maggio 2018, data in cui si applicherà obbligatoriamente il GDPR, continueranno a trovare applicazione per le parti non in contrasto con la normativa europea.

CAPO I – DISPOSIZIONI GENERALI

Art. 1 – Definizioni

Il presente regolamento si avvale delle seguenti definizioni:

- “Codice”: D.Lgs. n. 196/2003;
- “GDPR”: il 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 (GDPR generale sulla protezione dei dati);
- “Regolamento”: il presente Regolamento;
- “titolare”: il Comune o l'Amministrazione che adotta il presente regolamento, Comune di Cermenate con sede in Cermenate Via Scalabrini n. 153
- “dirigenti/P.O.”: i soggetti che esercitano i poteri delegati dal titolare o che sono nominati dal titolare per esercitare tali poteri.

Il presente regolamento recepisce le definizioni del D.Lgs. n. 196/2003 e del GDPR, fermo restando che, in caso di discordanza, prevalgono le definizioni contenute nei rispettivi testi normativi:

A) definizioni:

- “trattamento”: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- “dato personale”: 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 identificativi”: i dati personali che permettono l'identificazione diretta dell'interessato;
- “dati particolari”: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati,

associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

- “dati giudiziari”: i dati personali idonei a rivelare provvedimenti di cui all’articolo 3, comma 1, lettere da a) a o), e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- “Titolare”: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- “Responsabile ”: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti al trattamento di dati personali;
- “incaricati”: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile; “interessato”: la persona fisica, cui si riferiscono i dati personali;
- “comunicazione”: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- “diffusione”: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- “dato anonimo”: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- “blocco”: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- “banca di dati”: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- “Garante”: l’autorità di cui all’articolo 153 D.Lgs. 196/2003, istituita dalla legge 31 dicembre 1996, n. 675;
- “comunicazione elettronica”: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;
- “chiamata”: la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;
- “reti di comunicazione elettronica”: i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- “rete pubblica di comunicazioni”: una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;
- “servizio di comunicazione elettronica”: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall’articolo 2, lettera c), della direttiva 2002/21/ CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- “contraente”: qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

- “utente”: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- “dati relativi al traffico”: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- “dati relativi all’ubicazione”: ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell’apparecchiatura terminale dell’utente di un servizio di comunicazione elettronica accessibile al pubblico;
- “servizio a valore aggiunto”: il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all’ubicazione diversi dai dati relativi al traffico, oltre a quanto e’ necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- “posta elettronica”: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell’apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;
- “misure minime”: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell’articolo 31 D.Lgs.n. 196/2003;
- “strumenti elettronici”: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- “autenticazione informatica”: l’insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell’identità;
- “credenziali di autenticazione”: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l’autenticazione informatica;
- “parola chiave”: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- “profilo di autorizzazione”: l’insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa puo’ accedere, nonché i trattamenti ad essa consentiti;
- “sistema di autorizzazione”: l’insieme degli strumenti e delle procedure che abilitano l’accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
- “violazione di dati personali”: violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l’accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico;
- “scopi storici”: le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- “scopi statistici”: le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- “scopi scientifici”: le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore;
- “trattamenti effettuati per finalità amministrativo-contabili”: i trattamenti connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all’adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all’applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro;
- “profilazione”: qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l’affidabilità, il comportamento, l’ubicazione o gli spostamenti di detta persona fisica; “pseudonimizzazione”: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni

aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- “destinatario”: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- “stabilimento principale”:

- a) per quanto riguarda un Titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua Amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

- b) con riferimento a un Responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua Amministrazione centrale nell'Unione o, se il Responsabile del trattamento non ha un'Amministrazione centrale nell'Unione, lo stabilimento del Responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del Responsabile del trattamento nella misura in cui tale Responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

- “autorità di controllo”: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;

- “trattamento transfrontaliero”: - trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del trattamento o Responsabile del trattamento nell'Unione ove il Titolare del trattamento o il Responsabile del trattamento siano stabiliti in più di uno Stato membro;

oppure

- trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare del trattamento o Responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

Art. 2 – Quadro normativo di riferimento

Il presente Regolamento tiene conto dei seguenti documenti:

- Codice in materia di dati personali (D.Lgs. n. 196/2003);
- Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. n.196 del 30 giugno 2003);
- Linee guida e raccomandazioni del Garante;
- GDPR UE 679/2016 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;
- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (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;
- D.Lgs. n. 101 del 10 agosto 2018 di adeguamento della normativa interna al GDPR;
- Linee-guida Adottate dal Gruppo di lavoro Art. 29 (ora sostituito da European Data Protection Board)

Art. 3 – Oggetto

Il presente Regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal titolare, nel rispetto di quanto previsto dal GDPR.

Il presente Regolamento sostituisce integralmente il Regolamento sui dati sensibili, approvato con deliberazione C.C. n. 48 in data 19.12.2005, e aggiornato con deliberazione C.C. n. 14 in data 28.03.2007, ferme restando le schede/tabelle allegate al Regolamento medesimo, che identificano i tipi di dati particolari e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite nei singoli casi ed espressamente elencate dalla legge, le quali continuano ad applicarsi e vengono allegate al presente Regolamento per farne parte integrante e sostanziale.

Art. 4 – Finalità

Il titolare garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.

Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza del titolare, vanno gestiti conformemente alle disposizioni del Codice, del GDPR, e del presente Regolamento.

CAPO II – PRINCIPI

Art. 5 – Principi e responsabilizzazione

Vengono integralmente recepiti, nell'ordinamento interno del titolare, i principi del GDPR, per effetto dei quali dati personali sono:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei 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 ("limitazione della finalità");
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati base del principio di "minimizzazione dei dati";
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati base del principio di "esattezza";
- e) conservati in una forma che consenta l'identificazione degli interessati 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 a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "limitazione della conservazione";
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali in base ai principi di "integrità e riservatezza";
- g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo in un caso di necessità ("principio di necessità").

Il titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di provarlo in base al principio di "responsabilizzazione".

Art. 6 – Liceità del trattamento

Vengono integralmente recepiti, nell'ordinamento interno del titolare, le disposizioni del GDPR in ordine alla liceità del trattamento e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri¹ di cui è investito il Titolare del trattamento;

¹ Si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

- a) accesso a documenti amministrativi e accesso civico;
- b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
- c) tenuta di registri pubblici relativi a beni immobili o mobili;
- d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
- e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
- f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
- g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
- h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
- i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;
- l) attività di controllo e ispettive;
- m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- n) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;
- o) rapporti tra i soggetti pubblici e gli enti del terzo settore;
- p) obiezione di coscienza;
- q) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
- s) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
- t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;
- u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

f) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) non si applica al trattamento di dati effettuato dal titolare nell'esecuzione dei propri compiti e funzioni.

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri, che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 GDPR², al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Titolare tiene conto, tra l'altro:

- a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;

v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

2 1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;

f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;

g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;

h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);

i) la tutela dell'interessato o dei diritti e delle libertà altrui;

j) l'esecuzione delle azioni civili.

- c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del GDPR³, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10⁴ del medesimo GDPR;
- d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art. 7 – Condizioni per il consenso

Il consenso al trattamento dei dati non è richiesto al Comune di Cermenate in quanto pubblica amministrazione se agisce per finalità istituzionali.

Il consenso deve essere richiesto se il Comune agisce per specifiche finalità diverse da quelle istituzionali. In tal caso il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.

La richiesta di consenso deve essere comprensibile, facilmente accessibile, chiara e semplice.

Qualora il trattamento sia basato sul consenso, il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di apposita modulistica, predisposta dal titolare, previa consegna e presa d'atto dell'informativa.

Non è ammesso il consenso tacito o presunto ovvero l'utilizzo di caselle presunte su un modulo.

Il titolare adotta misure organizzative adeguate a facilitare l'espressione del consenso da parte dell'interessato.

La manifestazione del consenso, ad opera dell'interessato, va resa al momento del primo accesso alle prestazioni, ed è valido ed efficace fino alla revoca della stessa o, per i minorenni, fino al compimento del diciottesimo anno di età.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del DGPR e del presente regolamento è vincolante.

Per i dati particolari il consenso deve essere esplicito e in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;

Il consenso dei minori è valido a partire dai 16 anni, fermo restando il diverso limite di età, comunque non inferiore a 13 anni, previsto dalla normativa nazionale; prima di del limite età previsto dalla normativa nazionale occorre raccogliere il consenso dei genitori o di chi ne fa le veci; In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.

Il consenso viene registrato e conservato nel fascicolo relativo alla pratica trattata.

3 Articolo 9 - Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati Garante per la protezione dei dati personali biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

4 Articolo 10 - Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Il consenso può essere revocato ed in tal caso la revoca non pregiudica la liceità del trattamento già effettuato.

Art. 8 – Informativa

Prima che inizi qualunque trattamento di dati personali il Titolare del trattamento fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti.

L'informativa privacy deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.

Essa va effettuata:

- in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;
- in caso di dati personali non ottenuti presso l'interessato:
 - entro un termine ragionevole, massimo di un mese dalla raccolta (non registrazione) dei dati;
 - nel caso in cui i dati vadano comunicati all'interessato, alla prima comunicazione;
 - se i dati personali devono essere comunicati ad un altro destinatario, non oltre la prima comunicazione.

Non è necessario fornire l'informativa:

- nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;
- nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.

L'informativa è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
- avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il titolare;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incarico del trattamento dei dati relativi alle procedure.

L'informativa da fornire agli interessati può essere fornita anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

L'informativa contiene il seguente contenuto minimo:

- l'identità e i dati di contatto del titolare e, ove presente, del suo rappresentante;
- i dati di contatto del RPD/DPO ove esistente;
- le finalità del trattamento;
- i destinatari dei dati;
- la base giuridica del trattamento;
- l'interesse legittimo del titolare se quest'ultimo costituisce la base giuridica del trattamento;
- se il titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;

- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- il diritto dell'interessato di chiedere al titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
- il diritto di presentare un reclamo all'autorità di controllo;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

Nel caso di dati personali non raccolti direttamente presso l'interessato:

a) il titolare deve informare l'interessato in merito a:

- le categorie di dati personali trattati;
- la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico;

b) l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del titolare è predisposta apposita informativa per personale dipendente.

Apposite informative devono essere inserite nei seguenti documenti:

- nei bandi e nella documentazione di affidamento dei contratti pubblici, nei contratti, accordi o convenzioni, nei bandi di concorso pubblico, nelle segnalazioni di disservizio e, più in generale, in ogni altro documento contenente dati personali.

Nel fornire l'informativa, il titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati particolari e giudiziari.

Art. 9 – Sensibilizzazione e formazione

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del titolare e l'attività informativa diretta a tutti coloro che hanno rapporti con il titolare.

Per garantire la conoscenza capillare delle disposizioni del presente Regolamento, al momento dell'ingresso in servizio è data a ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale, con i riferimenti per l'acquisizione del presente Regolamento, pubblicato sul sito del titolare.

Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni. Il titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata, a cura del RPC, con la formazione in materia di prevenzione della corruzione e della illegalità nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il titolare.

CAPO III – IL TRATTAMENTO DEI DATI PERSONALI

Art. 10 – Trattamento dei dati personali, ricognizione dei trattamenti e indice dei trattamenti

Il titolare tratta i dati personali per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Codice, dal GDPR e dalle Linee Guida e dai provvedimenti del Garante.

Il titolare effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

- la gestione del personale dipendente, ivi comprese le procedure di assunzione;
- la gestione dei soggetti che intrattengono rapporti giuridici con il titolare, diversi dal rapporto di lavoro dipendente, e che operano a qualsiasi titolo all'interno della struttura organizzativa del titolare, ivi compresi gli stagisti, tirocinanti e i volontari;
- la gestione dei rapporti con i consulenti, i libero-professionisti, i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione lavori, opere e di interventi di manutenzione;
- la gestione dei rapporti con i soggetti accreditati o convenzionati per i servizi socio-assistenziali;
- la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del titolare, solo da parte dei soggetti appositamente autorizzati:

- titolare
- dirigenti/P.O., in qualità di soggetti che esercitano i poteri delegati dal titolare o in qualità di soggetti nominati dal titolare per l'esercizio di tali poteri
- dipendenti, in qualità di incaricati del trattamento.

Non è consentito il trattamento da parte di persone non autorizzate.

Ai fini del trattamento, il titolare provvede, in collaborazione con i dirigenti/P.O., alla integrale ricognizione e all'aggiornamento di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti del titolare medesimo, funzionali alla formazione dell'indice dei trattamenti. È compito dei dirigenti/P.O. effettuare e documentare l'aggiornamento periodico, almeno annuale, della ricognizione dei trattamenti e del relativo indice; la valutazione periodica, infrannuale del rispetto dei principi del presente Regolamento con riferimento a tutti trattamenti inclusi nell'indice verrà effettuato dal D.P.O./R.D.P.

L'elenco dei trattamenti deve essere comunicato annualmente al D.P.O./R.D.P., o su richiesta, in occasione delle verifiche infrannuali.

Il titolare, i dirigenti/P.O. e gli incaricati si attengono alle modalità di trattamento indicate nel Codice, nel GDPR, nonché nelle disposizioni attuative e nelle Linee guida del Garante per la protezione dei dati personali.

Art. 11 – Tipologie di dati trattati

Nell'ambito dei trattamenti inclusi nell'indice dei trattamenti, il titolare, nell'esercizio delle sue funzioni istituzionali, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati comuni identificativi
- dati particolari
- dati giudiziari.

Art. 12 – Trattamento dei dati particolari e giudiziari

I dati personali particolari, individuati dall'articolo 9 del G.D.P.R. sono:

- l'origine razziale ed etnica
- le convinzioni religiose, filosofiche o di altro genere
- le opinioni politiche
- l'adesione ai partiti, sindacati, associazioni o organizzazioni a carattere religioso, politico o sindacale
- lo stato di salute e la vita sessuale

Possono essere oggetto di trattamento nei seguenti casi, ai sensi dell'art 9⁵ GDPR :

- solo se autorizzati da espressa disposizione di legge che preveda i tipi di dati trattabili, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguibile;
- per lo svolgimento di attività per le quali in ragione delle rilevanti finalità di interesse pubblico perseguite sia intervenuta, a richiesta del soggetto pubblico interessato, apposita autorizzazione del Garante.

Il titolare conforma il trattamento dei dati particolari e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

Il titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati particolari e giudiziari.

I dati particolari possono essere comunicati ad altri soggetti pubblici e/o privati nei seguenti casi :

- quando la comunicazione è prevista da un'espressa norma di legge statale o regionale o da altra fonte equiparata
- quando la richiesta della comunicazione è avanzata da altro soggetto pubblico per il perseguimento di finalità che per legge o per il proprio ordinamento sono considerate di rilevante interesse pubblico; in tal caso, il richiedente deve indicare, per iscritto, la finalità perseguita e la disposizione di legge o del proprio ordinamento che attribuisce alla medesima il carattere di

-
- 5 a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
- b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
- c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
- e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniquale volta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali;
- g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
- i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
- j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

rilevante interesse pubblico. Della comunicazione dei dati è data notizia al Titolare ed al Responsabile dei dati medesimi;

- quando la richiesta è avanzata da un soggetto privato per far valere, innanzi all'Autorità Giudiziaria (penale, civile, amministrativa), un proprio diritto purché sia dimostrabile l'esistenza di un procedimento in corso;
- nel caso di ordine di esibizione e/o comunicazione dell'Autorità Giudiziaria.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono trattati da soggetti adeguatamente formati e sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

Art. 13 – Trattamento dei dati particolari all'interno del Comune

I dati particolari non devono assolutamente essere né divulgati né portati a conoscenza di chiunque.

I dati personali particolari possono esser oggetto di trattamento preferibilmente con il consenso scritto dell'interessato.

Gli Incaricati del trattamento dei dati particolari devono :

- acquisire preferibilmente il consenso al trattamento dei dati per iscritto
- consegnare l'informativa con evidenziati i diritti dell'interessato
- provvedere ad attuare le misure minime di sicurezza per la salvaguardia dei dati

Art. 14 – Trattamento dei dati del personale

Il titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo.

Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.

Secondo la normativa vigente, il titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica.

Il trattamento dei dati particolari del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo dei dati giudiziari e particolari, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici. Non sono infatti ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.

Il titolare, nel trattamento dei dati particolari relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.

Il titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 15 – Rilevanza delle schede/tabelle identificative delle tipologie di tipi di dati particolari e giudiziari per cui è consentito il relativo trattamento

Le schede identificative delle tipologie di dati particolari e giudiziari per cui è consentito il relativo trattamento da parte del titolare, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico:

- a) vanno consegnate, personalmente, agli incaricati a cui, in materia o competenza, si riferiscono;
- b) costituiscono oggetto di formazione;
- c) costituiscono oggetto di interventi di monitoraggio e di verifica con riguardo alla loro applicazione.

Art. 16 – Registro delle attività di trattamento e delle categorie di trattamento

Il responsabile di trattamento tiene registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
- c) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 GDPR.⁶
- e) le finalità di trattamento
- f) una descrizione delle categorie di interessati e delle categorie dei dati personali;
- g) la categorie di destinatari, a cui i dati personali sono o saranno comunicati;
- h) l'indicazione delle cautele specifiche, a cui ciascun Responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;
- i) un'eventuale possibilità di trasferimenti di dati all'estero;
- l) una descrizione generale delle misure di sicurezza, generiche e specifiche, così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali;
- m) indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

Su richiesta, il titolare del trattamento o il responsabile del trattamento, mettono il registro a disposizione del Garante.

⁶ Articolo 32 - Sicurezza del trattamento

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

CAPO IV – DIRITTI DEGLI INTERESSATI

Art. 17 – Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

Il Titolare, in sede di pubblicazione e diffusione, tramite l'albo pretorio informatico e la rete civica, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:

- a) sicurezza
- b) completezza
- c) esattezza
- d) accessibilità
- e) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.

Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, tranne deroghe previste da specifiche disposizioni.

Salva diversa disposizione di legge, il titolare garantisce la riservatezza dei dati particolari in sede di pubblicazione all'Albo on line o sulla rete civica, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.

In ogni caso, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere sensibile o giudiziario dell'interessato, devono essere anonimizzati con adeguate tecniche di anonimizzazione da valutare in base alle tecniche allo stato dell'arte.

Il titolare si conforma alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.

La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali

Art. 18 – Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati particolari e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.

Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Il titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

Art. 19 – Diritti dell'interessato

Il titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, di seguito elencati, in conformità alla disciplina contenuta nel GDPR e nel Codice.

Art. 20 – Diritto di accesso

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di accesso secondo la quale l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di Paesi terzi o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- f) il diritto di proporre reclamo a un'autorità di controllo;
- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1⁷ e 4⁸ GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.

Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Art. 21 – Diritto alla rettifica e cancellazione

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di rettifica e cancellazione («diritto all'oblio»), di seguito indicata.

Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Il titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

7 Articolo 22 - Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

8 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Quanto al diritto "all'oblio", consistente nel diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i)⁹, e dell'articolo 9, paragrafo 3¹⁰ GDPR;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1¹¹ GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 22 – Diritto alla limitazione

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto alla limitazione, e di seguito indicata.

L'interessato ha il diritto di ottenere dal titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:

- a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati personali;
- b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

9 h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

10 3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di Garante per la protezione dei dati personali e segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

11 Articolo 89 - Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1¹² GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18¹³ GDPR, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare prima che detta limitazione sia revocata.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 23 – Diritto alla portabilità

Il diritto alla portabilità dei dati di cui all'articolo 20 del G.D.P.R. non si applica ai trattamenti svolti dal Comune necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso ente.

Art. 24 – Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR¹⁴, compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede

12 Articolo 21 - Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

13 Articolo 18 - Diritto di limitazione di trattamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

- a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

14 Articolo 6 - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

giudiziaria. Il diritto di cui ai paragrafi 1 e 2 dell'art. 21¹⁵ GDPR è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del GDPR¹⁶, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Art. 25 – Modalità di esercizio dei diritti dell'interessato

Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR, del Codice e del presente Regolamento.

La richiesta per l'esercizio dei diritti può essere fatta pervenire:

- direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;
- tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;
- tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;
- in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;
- dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.

L'interessato può presentare o inviare la richiesta di esercizio dei diritti:

- al titolare o Responsabile del trattamento, che conserva e gestisce i dati personali dell'interessato;
- all'ufficio protocollo generale del titolare o all'ufficio per le relazioni con il pubblico.

La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento:

- alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.

Fermo restando l'accesso ai dati personali, il dirigente/P.O. autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.

I soggetti competenti alla valutazione dell'istanza sono:

15 Articolo 21 - Diritto di opposizione

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

16 Articolo 89 - Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

- il dirigente/P.O. competente;
il quale decide sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.
All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa.
I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.
L'accesso dell'interessato ai propri dati personali:
- può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del titolare.
L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.
Il titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Art. 26 – Indagini difensive

Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-quater del Codice di procedura penale, può chiedere documenti in possesso del titolare, e può estrarne copia, anche se contengono dati personali di un terzo interessato.
Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile rinviando, per ogni altro e ulteriore aspetto, alla relativa disciplina al Regolamento del titolare sul diritto di accesso.
Il titolare si conforma alle Linee guida del Garante in tema di indagini difensive.

CAPO V – SOGGETTI

Art. 27 – Titolare e contitolari

Il titolare del trattamento è il Comune di CERMENATE, rappresentato dal Sindaco pro tempore, in qualità di legale rappresentante del titolare, con sede in via Scalabrini n. 153, Cermenate.
Il titolare provvede:
- a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Codice, al GDPR e al presente Regolamento;
- a nominare, con proprio atto, i dirigenti/P.O. per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti, e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi, le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
- a formare e aggiornare l'elenco dei dirigenti/P.O., delegati o nominati, e a pubblicarlo sul sito web istituzionale del titolare;
- a designare, con proprio atto, il Responsabile per la protezione dei dati personali;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
- a favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
- a favorire l'adesione a meccanismi di certificazione;
- ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.
Il segretario comunale collabora con il Sindaco pro-tempore per l'attuazione degli adempimenti di cui sopra.

La contitolarità di cui all'art. 26 GDPR si realizza 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, quando due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento.

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. Tale accordo può designare un punto di contatto per gli interessati. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati.

Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo interno, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Art. 28 – Responsabili di Posizione organizzativa-P.O.

Il titolare conferisce i sotto indicati compiti e funzioni, e i correlati poteri, ai Responsabili di P.O. Nel suddetto provvedimento, il titolare deve informare ciascun Responsabile di P.O. delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento.

Compiti, funzioni e poteri:

- trattare i dati personali solo su istruzione del titolare del trattamento;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare il tempestivo ed integrale rispetto dei doveri del titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32¹⁷ del GDPR;
- osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal titolare;
- adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;
- collaborare con il titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in

17 Articolo 32 - Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
 - a) la pseudonimizzazione e la cifratura dei dati personali;
 - b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo 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.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

collaborazione con l'amministratore di sistema e con le altre strutture competenti del titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;

- curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del titolare per l'applicazione del Codice, del GDPR, e del presente Regolamento;

- assistere il titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;

- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR¹⁸ (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;

- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, GDPR e nel presente Regolamento;

- contribuire alle attività di verifica del rispetto del Codice, del GDPR e del presente regolamento, comprese le ispezioni, realizzate dal titolare o da un altro soggetto da questi incaricato;

- curare la costituzione e l'aggiornamento dei seguenti archivi/banche dati, per quanto di competenza:

- elenco dei contitolari, dei responsabili dei trattamenti, e degli incaricati, con i relativi punti di contatto;

- elenco degli archivi/ banche dati;

- garantire l'aggiornamento, almeno annuale, della ricognizione dei trattamenti;

- fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

Ciascun Responsabile di P.O. risponde al titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.

I Responsabili di P.O. sono destinatari degli interventi di formazione di aggiornamento.

Art. 29 – Responsabili del trattamento e sub responsabili

E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub- responsabile.

Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

¹⁸ Articolo 32 - Sicurezza del trattamento

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato

Articolo 35 - Valutazione d'impatto sulla protezione dei dati

Articolo 36 - Consultazione preventiva

Art. 30 – Incaricati esterni del trattamento

Il titolare può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali, può designare quali Responsabili del trattamento dei dati personali, unicamente i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato (GDPR, art. 28)¹⁹.

Art. 31 – Responsabili del trattamento non dipendenti del titolare

Tutti i soggetti che svolgono un'attività di trattamento dei dati, e che non sono dipendenti del titolare, quali a titolo meramente esemplificativo i tirocinanti, i volontari e i soggetti che operano temporaneamente all'interno della struttura organizzativa del titolare o incaricati nominati dal Responsabile esterno), devono essere incaricati del trattamento tramite atto scritto di nomina.

Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli incaricati dipendenti del titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

19 Articolo 28 - Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
 2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
 3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
 - a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
 - b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
 - c) adotti tutte le misure richieste ai sensi dell'articolo 32;
 - d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
 - e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
 - f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
 - g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.
- Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Gli incaricati non dipendenti dal titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 32 – Amministratore di sistema

L'amministratore di sistema, individuato nel Responsabile del Centro Elaborazione Dati, sovrintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione. La nomina dell'amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. L'amministratore di sistema svolge attività, quali:

- il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.

Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema:

- deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici.

Le registrazioni (access log) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.

Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato, con cadenza annuale, da parte del titolare del trattamento coadiuvato dal D.P.O., in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.

L'amministratore di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

L'amministratore di sistema è destinatario degli interventi di formazione di aggiornamento.

Art. 33 – Responsabile della protezione dei dati personali (RPD) – Data Protection Officer (DPO)

Il Titolare designa il Responsabile della protezione dei dati (RPD/DPO).

Il RPD/DPO deve essere in possesso di:

- un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.

Il RPD/DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.

Il RPD/DPO svolge i seguenti compiti:

- informa e fornisce consulenze al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
- verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
- fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti. Il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante;

- funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
- funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Responsabili di Settore/Servizi che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:

- a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

CAPO VI – SICUREZZA DEI DATI PERSONALI

Art. 34 – Misure di sicurezza

Il titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

In particolare il titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate per garantire un livello di sicurezza adeguato al rischio. Tali misure che comprendono almeno:

- la pseudonimizzazione e la cifratura dei dati personali trattati;
- procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Per quanto attiene al trattamento dei dati personali effettuato con strumenti elettronici e non, il titolare applica le misure minime di sicurezza ritenute adeguate in riferimento al proprio contesto, come previsto dall'art. 32 del GDPR.

È fatto divieto al personale di consentire ad Amministratori, Cittadini ed altre persone non autorizzate per iscritto dal/i Responsabile/i o dal Titolare di utilizzare gli strumenti informatici, personal computer o videotermini, installati negli uffici.

Gli accessi ai dati, tramite computer, devono essere protetti da password ed è fatto divieto di renderle pubbliche o comunicare ad altri le proprie password personali di accesso ai dati.

La gestione delle password di accesso alla rete informatica dovrà essere strutturata per permettere la loro sostituzione automatica ogni 90 giorni.

I documenti cartacei contenenti dati personali devono essere conservati in archivi ad accesso controllato e con possibilità di chiusura.

I documenti cartacei contenenti dati particolari dovranno essere conservati con modalità che ne impediscano la diretta visione ed in armadi chiudibili a chiave.

È fatto divieto al personale non autorizzato di accedere ai locali dell'Ufficio Elaborazione Dati.

È fatto obbligo al personale dipendente di adeguarsi a tali norme e di utilizzare esclusivamente la modulistica adottata.

Art. 35 – Valutazione d'impatto sulla protezione dei dati DPIA

La valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

La DPIA è uno strumento importante per la responsabilizzazione in quanto sostiene il titolare non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo GDPR.

La DPIA sulla protezione dei dati personali deve essere realizzata, prima di procedere al trattamento, dal titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, intendendosi per "rischio" uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità, e per "gestione dei rischi" l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

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 GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

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.

Ricorrono rischi elevati ai sensi dell'art. 35, par. 3, lett. a)-c) Reg. UE 679/2016 in presenza di:

- una valutazione sistematica di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quali si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su tali persone fisiche;
- trattamento su larga scala, di categorie particolari di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, relativi alla salute, alla vita sessuale o condanne penali, a reati e misure di sicurezza;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il Comune altresì redige una valutazione di impatto del rischio se ricorrono due dei seguenti indici forniti dal Garante:

- valutazione o assegnazione di un punteggio inclusiva di profilazione, in particolare in considerazione di 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;
- dati particolari o di carattere altamente personale;
- trattamento di dati su larga scala;
- creazione di corrispondenze o combinazione di insiemi di dati;
- dati relativi a interessati vulnerabili considerato lo squilibrio di potere tra gli interessati ed il Comune;
- uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

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.

La DPIA non è richiesta nei seguenti casi:

- quando, sulla base di predetti criteri, risulta che il trattamento non è tale da “presentare un rischio elevato per i diritti e le libertà delle persone fisiche”;
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo;
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e)²⁰ GDPR, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10²¹ GDPR).

20 Articolo 6 - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

21 Articolo 35 - Valutazione d'impatto sulla protezione dei dati

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il

Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

Art. 36 – Pubblicazione sintesi della valutazione d'impatto – DPIA

Il titolare effettua la pubblicazione della DPIA o di una sintesi della stessa al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare, nonché di dimostrare la responsabilizzazione e la trasparenza.

La DPIA pubblicata non deve contenere l'intera valutazione qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il titolare o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

Art. 37 – Consultazione preventiva

Nei casi in cui si è proceduto nella valutazione di impatto sulla protezione dei dati ed è emerso che il Comune non riesce a trattare in maniera sufficiente tutti i rischi elevati, poiché ne restano ancora alcuni per questi ultimi residui, va consultato preventivamente il Garante per la privacy.

Il Comune di Cermenate, tramite il Responsabile della protezione dei dati, ai sensi degli artt. 36 e 39, par. 1, lett. e), Regolamento UE n. 679/2016, invia richiesta di consultazione al Garante comunicando:

- i dati dell'ente locale in quanto Titolare del trattamento ed i propri dati in quanto punto di contatto e referente per la consultazione;
- le finalità ed i mezzi di trattamento previsti;
- le misure di garanzia previste per proteggere i diritti e le libertà fondamentali degli interessati;
- la valutazione di impatto -sulla protezione dei dati in versione completa;
- ogni altra informazione ritenuta necessaria.

Il Garante formula parere scritto entro otto settimane²² dal ricevimento della richiesta di consultazione nel caso in cui ritenga che il trattamento comunicato violi le norme sulla protezione dei dati ed in particolare qualora ritenga che il Comune non abbia sufficientemente attenuato o identificato il rischio. In base alla complessità del trattamento previsto il Garante può prorogare la sua risposta di un termine aggiuntivo di sei settimane informando il Responsabile della protezione dei dati, entro un mese dal ricevimento della richiesta di consultazione.

In caso sia necessario il Garante può richiedere al Responsabile della protezione dei dati informazioni aggiuntive a quelle già comunicate e può sospendere la decorrenza dei termini di cui al comma 3 in attesa della loro trasmissione.

In assenza di parere espresso del Garante entro le otto settimane dal ricevimento della richiesta di consultazione, il Comune può procedere nel trattamento dei dati.

Art. 38 – Modulistica e procedure

Il titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del GDPR, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante

- a) adotta e costantemente aggiorna:
- modelli uniformi di informativa;

trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

²² Art. 36 GDPR

- modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;
- b) elabora, approva, e costantemente aggiorna:
- adeguate procedure gestionali da raccogliere in un apposito repository digitale.

Art. 39 – Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è sanzionato con le sanzioni previste dagli articoli 83 e 84 G.D.P.R. da parte del Garante, nonché con sanzioni di natura disciplinare.

Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.

Il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi previsti nel Codice nel GDPR e nel presente regolamento, e a lui specificamente diretti o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal titolare del trattamento.

Il titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 40 – Notificazione di una violazione dei dati personali

La violazione dei dati personali è una violazione di sicurezza che comporta accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali.

Per distruzione non autorizzata è da intendersi un'azione che rende irreversibile il processo di ricostruzione del dato personale determinando la sua esatta e totale eliminazione in rerum natura.

Per perdita è da intendersi la fuoriuscita del dato trattato ai fini di privacy dalla sfera del legittimo detentore in modo del tutto incontrollato e non tracciato.

Per modifica non autorizzata è da intendersi una deficienza organizzativa o fatti illeciti che, incidendo sulla conformazione del dato, è capace di arrecare danni fisici e morali agli interessati (es. si pensi nel mondo della sanità a casi di sostituzioni errate di terapie).

Per rivelazione non autorizzata è da intendersi la comunicazione di un segreto professionale.

Per accesso non autorizzato è da intendersi l'illecita attività di terzi (hacker) capaci di sottrarre e disporre di dati di un sistema attaccato grazie a particolari tecniche elusive di protezione.

Per soggetto non autorizzato è da intendersi ogni persona diversa da quella competente nell'ente a possedere e trattare i dati.

Il Responsabile del trattamento in caso venga a conoscenza della violazione informa senza ingiustificato ritardo il Titolare del trattamento e richiede immediato parere al Responsabile della protezione dei dati sulla gravità della violazione, ovvero:

- se questa sia inoffensiva per le misure di sicurezza già presenti in questo ente;
- se può comportare rischi per gli interessati al trattamento ed il grado dei rischi;
- le misure di sicurezza eventualmente da adottare per porre rimedio alla violazione.

Il Responsabile del trattamento relaziona immediatamente al Titolare del trattamento la violazione indicando la categoria di dati violati ed allega il parere del Responsabile della protezione dei dati in cui viene indicato se le misure presenti nel Comune rendono la violazione inoffensiva o, se invece, vanno integrate.

Al Titolare del trattamento compete, previa acquisizione del parere del DPO, la valutazione finale sulla gravità o meno della violazione. In caso venga riscontrata la presenza di rischi per le persone fisiche va effettuata via Pec la notifica della violazione al Garante per la privacy entro 72 ore dal momento in cui ne è venuto a conoscenza o, se in un momento successivo, nel provvedimento vanno indicati i motivi del ritardo.

La Notifica al Garante non è necessaria se la violazione è inoffensiva, cioè vi è assenza di rischio per interessati persone fisiche e ciò si verifica se il Comune al momento in cui essa si è verificata aveva misure di sicurezza che hanno reso i dati inintelligibili perché per esempio anonimi o cifrati in modo sicuro attraverso un algoritmo standardizzato o mediante schemi di cifratura a chiave simmetrica.

Non ricorre l'inintelligibilità se la violazione ha portato la distruzione o perdita dei dati personali.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Art. 41 – Comunicazione di una violazione dei dati personali

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

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).

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, 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).

La comunicazione all'interessato del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni:

- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali-

In caso non ricorrano i presupposti per la notifica al Garante come indicati dall'articolo precedente, non si procede nemmeno alla comunicazione all'interessato.

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

- a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
- c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Il Titolare del trattamento documenta ogni violazione dei dati personali, la procedura avviata internamente all'ente locale ed i provvedimenti per porvi rimedio. A tal fine redige apposita scheda tecnica cui sono allegati la relazione del Responsabile del trattamento ed il parere del RPD.

Il Titolare del trattamento annota, per il tramite del R.D.P., la violazione nel Registro delle violazioni, che contiene tra le altre informazioni: l'ufficio dell'ente locale competente al trattamento dei dati violati, la descrizione e la gravità della violazione, l'indicazione dei dispositivi cartacei o automatizzati coinvolti, la categoria dei dati violati e dei destinatari, le misure di sicurezza presenti ed applicate ai dati violati e le ulteriori eventuali misure adottate.

La documentazione è a disposizione di eventuali ispezioni e verifiche da parte del Garante privacy.

Art. 42 – Disposizioni finali

Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, le Linee guida e i provvedimenti del Garante.

Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.