



**CITTÀ DI CARINI**  
PROVINCIA DI PALERMO

# **REGOLAMENTO INTERNO PER LA PROTEZIONE DEI DATI PERSONALI NEL COMUNE DI CARINI**

*ai sensi del Regolamento Europeo 2016/679, D. Lgs. n.196/2003  
modificato dal D. Lgs n.101/2018*

ALLEGATO ALLA DELIBERA N. \_\_\_\_\_ DEL. \_\_\_\_\_

## Sommario

Art. 1 -	QUADRO NORMATIVO DI RIFERIMENTO.....	3
Art. 2 -	DEFINIZIONI.....	4
Art. 3 -	OGGETTO.....	5
Art. 4 -	TRATTAMENTO DEI DATI DA PARTE DI UN'AMMINISTRAZIONE PUBBLICA.....	6
Art. 5 -	FINALITA'.....	6
Art. 6 -	LICEITA' DEL TRATTAMENTO.....	7
Art. 7 -	LE OPERAZIONI DI TRATTAMENTO.....	8
Art. 8 -	CONDIZIONI PER IL CONSENSO.....	8
Art. 9 -	TRATTAMENTO DEI DATI RELATIVI ALLA SALUTE.....	9
Art. 10 -	TRATTAMENTO DEI DATI DEL PERSONALE.....	9
Art. 11 -	TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI.....	10
Art. 12 -	TRATTAMENTO DATI PERSONALI PER CONDANNE PENALI E REATI.....	11
Art. 13 -	CATEGORIE DI DATI.....	11
Art. 14 -	INFORMATIVA.....	11
Art. 15 -	I SOGGETTI COINVOLTI NELLA PROTEZIONE DATI.....	13
15.1 -	TITOLARE DEL TRATTAMENTO.....	13
15.2 -	RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO).....	14
15.3 -	RESPONSABILI ESTERNI.....	16
Art. 16 -	CONTITOLARI DEL TRATTAMENTO.....	17
Art. 17 -	AMMINISTRATORE DI SISTEMA.....	17
Art. 18 -	PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI (DELEGATI – SUBDELEGATI/AUTORIZZATI).....	17
Art. 19 -	ISTRUZIONI DI CARATTERE GENERALE PER TUTTI GLI AUTORIZZATI AL TRATTAMENTO.....	18
Art. 20 -	L'INTERESSATO.....	19
20.1 -	DIRITTO DI ACCESSO DELL'INTERESSATO.....	19
20.2 -	DIRITTO DI RETTIFICA.....	20
20.3 -	DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO).....	20
20.4 -	DIRITTO DI LIMITAZIONE DEL TRATTAMENTO.....	20
20.5 -	OBBLIGO DI NOTIFICA IN CASO DI RETTIFICA O CANCELLAZIONE DEI DATI PERSONALI O LIMITAZIONE DEL TRATTAMENTO.....	21
20.6 -	DIRITTO ALLA PORTABILITÀ DEI DATI.....	21
20.7 -	DIRITTO DI OPPOSIZIONE.....	21
Art. 21 -	TRATTAMENTI DATI RELATIVI ALL'ATTIVITA' DI WHISTLEBLOWING.....	21
Art. 22 -	REGISTRO DELLE ATTIVITA' DI TRATTAMENTO.....	22
Art. 23 -	VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA.....	22
Art. 24 -	VIOLAZIONE DEI DATI PERSONALI – NOTIFICA E COMUNICAZIONE.....	23
Art. 25 -	SICUREZZA E CONSERVAZIONE DEI DATI.....	25
Art. 26 -	FORMAZIONE.....	26
Art. 27 -	ATTIVITÀ DI SENSIBILIZZAZIONE.....	26
Art. 28 -	PUBBLICAZIONE GRADUATORIE.....	26
Art. 29 -	PUBBLICAZIONE ALBO ON LINE.....	26
Art. 30 -	IL DIRITTO DI ACCESSO E IL DIRITTO ALLA RISERVATEZZA.....	26
Art. 31 -	PUBBLICAZIONE NELL'AMMINISTRAZIONE TRASPARENTE.....	27
Art. 32 -	UTILIZZO HARDWARE E SOFTWARE.....	27
Art. 33 -	UTILIZZO DELLA RETE.....	28
Art. 34 -	RILASCIO CREDENZIALI DI AUTENTICAZIONE.....	28
Art. 35 -	USO DELLA POSTA ELETTRONICA DELLA RETE INTERNET E DEI RELATIVI SERVIZI.....	28
Art. 36 -	RESPONSABILITÀ IN CASO DI VIOLAZIONE DELLE DISPOSIZIONI IN MATERIA DI PRIVACY.....	29
Art. 37 -	RINVIO A DISPOSIZIONI DI LEGGE.....	29

## PREMESSA

Il diritto alla privacy è un vero e proprio 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.

La principale novità introdotta dal Regolamento Europeo in materia di protezione dei dati personali 2016/679, noto anche come GDPR – General Data Protection Regulation, consiste nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio, in luogo del precedente approccio basato su adempimenti. La protezione dei dati è rimessa al Titolare del Trattamento il quale, grazie al principio di responsabilizzazione (“accountability”), potrà, nei limiti e dentro i parametri delineati dal Regolamento, adottare le misure che ritiene più opportune e comprovare il conseguimento degli obiettivi che ha raggiunto nel rispetto dei principi che presiedono il trattamento dei dati personali.

Tutti coloro che a diverso titolo operano in nome e per conto del Comune di Carini e che trattano dati personali di terzi sono formalmente designati per svolgere le attività di trattamento, ricevono istruzioni operative e formazione specifica e sono chiamati al rigoroso segreto d'ufficio. Dette designazioni hanno luogo ad avvenuta esecutività del presente Regolamento, con riferimento al personale già in servizio, ovvero, per il personale di prossima assunzione, al momento dell'immissione in servizio e, nello specifico, su espresso mandato del Titolare al momento della sottoscrizione del rispettivo contratto individuale.

Altra importante finalità da perseguire è chiarire il corretto utilizzo della strumentazione elettronica che nel tempo – senza sostituire completamente le forme tradizionali e tipiche della sanità- ha preso piede nello scambio di informazioni. Si è valutato come i principi di efficienza ed efficacia che connotano la qualità delle prestazioni sanitarie non possano e non debbano mettere a rischio le libertà fondamentali di ciascuno.

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.

Il Titolare intende adeguare e conformare la propria normativa, regolamentare alle novità introdotte dal citato regolamento UE, fermo restando che il presente Regolamento e' 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.

## Art. 1 - QUADRO NORMATIVO DI RIFERIMENTO

Il Quadro normativo sulla quale si fonda il presente Regolamento sulla protezione dei dati del Comune di Carini, riguarda:

- Regolamento Europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con “GDPR”, Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati;
- D. Lgs. n. 196/2003 e ss.ii.mm. anche “Codice della Privacy”;
- D. Lgs. n.82/2005 “Codice Amministrazione digitale” successivamente modificato e integrato prima con il Decreto Legislativo 22/8/2016 n.179 e poi con il Decreto Legislativo 13/12/2017 n.217 per promuovere e rendere effettivi i diritti di cittadinanza digitale;
- Legge n.241/1990 “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi” e ss.mm.;
- Direttiva UE n. 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati;
- D. Lgs. 10/8/2018 n.101, recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27/4/2016, 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 (regolamento generale sulla protezione dei dati);
- Decreto del Presidente del Consiglio dei Ministri 8 agosto 2013;
- D. L. 08/10/2021 n° 139 convertito con modificazioni dalla L. 03/12/2021 n° 205 - Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali;
- Linee guida adottate dal Comitato europeo per la protezione dei dati (“European Data Protection Board”, EDPB), nonché dal precedente Gruppo di lavoro “Articolo 29” (WP29);
- Provvedimenti, linee guida e pareri emanati dall’Autorità Garante per la protezione dei dati personali;
- Regolamenti, policy, istruzioni operative nonché atti organizzativi, delibere e determine ed ogni altro documento interno all’Ente del Titolare del Trattamento che risulti funzionale al raggiungimento delle finalità della presente politica.

## Art. 2 - DEFINIZIONI

- 1) «**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;
- 2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- 4) «**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;

- 5) «**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;
- 6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- 7) «**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;
- 8) «**Titolare del Trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del Trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- 9) «**Responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del Trattamento;
- 10) «**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;
- 11) «**Terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del Trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 12) «**consenso dell'Interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- 13) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- 14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- 15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- 16) «**Codice**»: D.Lgs. n. 196/2003;
- 17) «**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);
- 18) «**Autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE 2016/679;
- 19) «**Autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il Titolare del Trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato

proposto a tale autorità di controllo;

Per le altre definizioni si rinvia all'art. 4 del Regolamento UE 2016/679.

### **Art. 3 - OGGETTO**

Il presente Regolamento ha ad oggetto la disciplina dell'ordinamento degli uffici e dei servizi comunali in attuazione del D. Lgs. n.196/03 (codice privacy) e del Regolamento UE 2016/679 (GDPR), con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Ente.

L'Ente adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. L'Ente adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'Interessato ai sensi dell'art.15 del Regolamento UE 2016/679.

Ed in particolare il presente Regolamento:

- a) individua i compiti del Titolare e dei Responsabili, nonché degli Autorizzati del trattamento dei dati personali esistenti e gestiti presso gli uffici comunali;
- b) disciplina il trattamento dei dati personali effettuato dall'Amministrazione comunale nello svolgimento dei propri compiti istituzionali.

### **Art. 4 – TRATTAMENTO DEI DATI DA PARTE DI UN'AMMINISTRAZIONE PUBBLICA**

Ai sensi dell'art. 9 del D. L. 08/10/2021 n° 139 convertito in legge con modificazioni dalla L. 3 dicembre 2021, n. 205, il trattamento dei dati personali da parte di un'Amministrazione Pubblica di cui all'art. 1, comma 2 del D. Lgs. 30/03/2001, n° 165, è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti. La finalità del trattamento, se non prevista da una norma di legge o di regolamento, è indicata dall'Amministrazione, assicurando adeguata pubblicità all'identità del Titolare del trattamento, alle finalità del trattamento e fornendo ogni altra informazione necessaria ad assicurare il trattamento corretto e trasparente con riguardo ai soggetti interessati, ai loro diritti di ottenere conferma e comunicazione di un trattamento dei dati personali che li riguardano.

La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste da una norma di legge o di regolamento o da atti amministrativi generali. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

Laddove fosse necessario procedere con un trattamento non previsto da una norma di legge o di regolamento, è necessario fare una richiesta specifica all'Ufficio Protezione dei dati secondo un'apposita procedura predisposta dal Titolare del trattamento nel rispetto dell'art. 5 del Regolamento UE 2016/679.

### **Art. 5 - FINALITA'**

Il Titolare del Trattamento 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 secondo i principi contenuti nel Regolamento UE 2016/679 in conformità alle norme del D. Lgs.196/2003, come modificato dal D. Lgs. del 10 agosto 2018 n.101 (Codice Privacy). Il titolare,

nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale. 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 del Trattamento, vanno gestiti conformemente alle disposizioni del Codice, del GDPR, e del presente Regolamento.

I trattamenti posti in essere dal Comune hanno le seguenti finalità:

1. l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:
  - l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
  - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
  - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale o regionale affidate al Comune in base alla vigente legislazione.
2. l'adempimento di un obbligo legale al quale è soggetto il Comune.;
3. 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;
4. per la salvaguardia degli interessi vitali dell'Interessato o di altra persona fisica;
5. l'Interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

I dati personali sono trattati dal Titolare del Trattamento in modo lecito, corretto e trasparente e sono raccolti per le finalità determinate dalla legge e dai regolamenti che sono esplicite e legittime, e i trattamenti avvengono in modo non incompatibile con le finalità istituzionali attribuite.

I dati sono trattati in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono trattati e di norma secondo il criterio di «minimizzazione dei dati». Dei dati è costantemente verificata l'esattezza e, quando è necessario l'aggiornamento. Nel trattamento il Comune di Carini, adotta tutte le misure tecniche adeguate e ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

## **Art. 6 - LICEITÀ DEL TRATTAMENTO**

Vengono integralmente recepiti, nell'ordinamento interno del Titolare del Trattamento, 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 poteri di cui è investito il Titolare del trattamento;

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 GDPR, 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;
- c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del GDPR, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 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 - LE OPERAZIONI DI TRATTAMENTO**

Per trattamento si intende qualunque operazione, o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali o insiemi di dati personali, come:

6. La raccolta dei dati;
7. La registrazione dei dati, ovvero il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
8. L'organizzazione dei dati, cioè il processo di lavorazione finalizzato a favorirne la fruibilità attraverso l'aggregazione, la disaggregazione, l'accorpamento, la catalogazione;
9. La conservazione dei dati;
10. L'adattamento o la modifica in relazione a variazioni o a nuove acquisizioni;
11. L'estrazione;
12. La consultazione;
13. L'uso;
14. La comunicazione, ovvero la trasmissione dei dati a uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; la comunicazione dei dati avviene solo nei casi previsti da norme di legge o regolamento;
15. La diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati (es. pubblicazione nell'albo pretorio, ecc)
16. La limitazione, cioè il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
17. La cancellazione;
18. La distruzione.

Le operazioni di trattamento possono essere effettuate solo dal Titolare del Trattamenti, dai Responsabili, da Delegati o dai sub-delegati/Autorizzati al Trattamento, di cui all'art.2-quaterdecies del Codice della Privacy, ovvero dai responsabili di cui all'art.28 del Regolamento UE 2016/679.

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

Il Responsabile della protezione dei dati (D.P.O.), nell'ambito dei compiti attribuiti e delle funzioni svolte nel rispetto del Regolamento UE 2016/679, può effettuare tutte le operazioni di trattamento connesse al ruolo ricoperto.

### **Art. 8 - CONDIZIONI PER IL CONSENSO**

Fermi restando i casi, disciplinati dalla normativa vigente, nei quali può essere legittimamente effettuato il trattamento senza consenso, nei casi in cui il trattamento dei dati personali, per una o più specifiche finalità, è subordinato al consenso dell'interessato, si applica l'art. 7 del Regolamento UE 2016/679, prevedendo che

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
2. 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 presente regolamento è vincolante;
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
  4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Inoltre, prima di esprimere il proprio consenso, l'Interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

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.

#### **Art. 9 - TRATTAMENTO DEI DATI RELATIVI ALLA SALUTE**

Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali relativi allo stato di salute. 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. 10 - TRATTAMENTO DEI DATI DEL PERSONALE**

Il Comune di Carini tratta i dati, anche di natura particolare 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, incluso i trattamenti 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, la definizione dello stato giuridico, del trattamento economico, degli obblighi retributivi, fiscali e contabili del personale in servizio o in quiescenza.

L'Ente come pubblica amministrazione può comunicare ad altre amministrazioni pubbliche i dati trattati quando la comunicazione dei dati ha base nella legge, come ai sensi del combinato disposto dell'art. 9, comma 1, della L. 16/1/2003 n. 3 e dell'art. 3, comma 61, della L. 24/12/2003 n. 350, richiamato dall'art. 1, comma 100, della L. n. 311/2004 gli enti locali, che nell'esercizio della propria potestà regolamentare, possono attingere previo accordo a graduatorie concorsuali ancora valide approvate da altre amministrazioni. La comunicazione può essere anche effettuata in esecuzione di compiti di interesse pubblico ai sensi dell'art. 2 sexies del D. Lgs. 196/2003 ovvero nell'esercizio del pubblico potere attribuito e per gli obblighi previsti e volti a tutelare le esigenze della legislazione fiscale, assistenziale e previdenziale.

La comunicazione dei dati a terzi è consentita in forma anonima e ai fini delle politiche del lavoro e di statistica ricavati dalle informazioni relative a singoli o a gruppi di lavoratori: come il numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate nelle varie articolazioni organizzative, gli importi di trattamenti stipendiali o accessori individuati per fasce o qualifiche/livelli professionali, le giornate non lavorate per motivi di salute, o per benefici di legge anche nell'ambito di singole funzioni o unità organizzative, salvo che anche tale diffusione di dati anonimi sia di pregiudizio per la libertà e dignità del lavoratore qualora individuabile.

Ad esclusione dei casi in cui il contratto collettivo applicabile preveda espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale per verificare la corretta attuazione di taluni atti organizzativi, l'amministrazione può fornire alle organizzazioni sindacali dati numerici o aggregati e non anche

quelli riferibili ad uno o più lavoratori individuabili. È il caso, ad esempio, delle informazioni inerenti ai sistemi di valutazione dell'attività dei dirigenti, alla ripartizione delle ore di straordinario e alle relative prestazioni, nonché all'erogazione dei trattamenti accessori.

L'amministrazione può anche rendere note alle organizzazioni sindacali informazioni personali relative alle ritenute effettuate a carico dei relativi iscritti, in conformità alle pertinenti disposizioni del contratto applicabile.

La pubblicazione delle graduatorie per la selezione di personale o per la concessione di benefici economici, agevolazioni o contributi, deve essere effettuata dopo avere verificato che le informazioni ivi contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute.

L'Ente gestisce il trattamento dei dati personali dei lavoratori relativi al rapporto di lavoro in ambito pubblico, nel rispetto di quanto previsto dalla legislazione vigente e dai Provvedimenti e dalle Linee Guida del Garante per la protezione dei dati personali.

### **Art. 11 - TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI**

Il Titolare del Trattamento non provvederà al trattamento dei dati "particolari" di cui all'art. 9 del GDPR e, in assenza di previsione derogatoria ovvero dell'espresso consenso dell'Interessato o da altre deroghe dopo specificate, il personale del Comune di Carini si astiene dal trattare dati "particolari" che direttamente o indirettamente siano idonei a far rilevare:

- ✓ l'origine razziale o etnica dei soggetti i cui dati vengono trattati;
- ✓ le loro opinioni politiche;
- ✓ le loro convinzioni religiose o filosofiche;
- ✓ l'appartenenza sindacale anche per i dipendenti interni;
- ✓ i loro dati genetici;
- ✓ i loro dati biometrici che identificano la persona fisica, dati relativi alla salute;
- ✓ alla vita sessuale o all'orientamento sessuale.

Quanto prima indicato non si applica qualora si verifichi uno dei seguenti casi:

- a) l'Interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- 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 riguarda dati personali resi manifestamente pubblici dall'Interessato;
- e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali;
- f) 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;
- g) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi e assistenza, sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale;
- h) il trattamento è necessario a fini di archiviazione nel pubblico interesse, ricerca storica o a fini statistici in

conformità dell'articolo 89 del Regolamento UE 2016/679 (GDPR), 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.

#### **Art. 12 - TRATTAMENTO DATI PERSONALI PER CONDANNE PENALI E REATI**

Il trattamento dei dati personali relativi a condanne penali e reati deve svolgersi secondo quanto previsto dell'art.10 del R.E. e dall'art.2 octies del Codice della Privacy n.196/2003. 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.

I dati particolari e giudiziari individuati nel presente regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'Interessato.

Le operazioni di interconnessione, raffronto, comunicazione e diffusione individuate nel presente regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o compiti di volta in volta indicati, per il perseguimento delle finalità di interesse pubblico specificate e nel rispetto delle disposizioni rilevanti in materia di protezione dei dati personali, nonché degli altri limiti stabiliti dalla legge e dai regolamenti. I dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali sono inutilizzabili.

#### **Art. 13 - CATEGORIE DI DATI**

Il Comune di Carini in qualità di Titolare del Trattamento, tratta dati di tipo personale e particolare relativi a:

1. utenti, cittadini e loro familiari e/o accompagnatori;
2. personale del Comune con rapporto di dipendenza, convenzione o collaborazione;
3. soggetti che per motivi di studio, tirocinio, consulenza, stage o volontariato frequentano le strutture dell'Ente ed effettuano trattamento di dati personali;
4. clienti e imprese che intrattengono rapporti con Il Comune di Carini per l'approvvigionamento di beni e servizi o per l'esecuzione di opere edilizie e interventi di manutenzione;
5. personale e imprese partecipanti a bandi, gare e selezioni.

I dati personali trattati dal Titolare del Trattamento nelle forme e nei limiti di quanto previsto dalla vigente normativa sono raccolti:

- ✓ prioritariamente presso l'Interessato o anche presso persone diverse nei casi in cui questi sia minorenni o incapace o non sia in grado di fornirli;
- ✓ anche presso altri enti e amministrazioni pubbliche o terzi, presso pubblici registri o presso altri esercenti le professioni sanitarie;
- ✓ anche presso banche dati nazionali o regionali di libero accesso o ad accesso riservato.

#### **Art. 14 - INFORMATIVA**

Il Comune di Carini in qualità di Titolare del Trattamento, adotta misure appropriate per fornire all'Interessato tutte le informazioni e comunicazioni riguardanti il trattamento dei dati quali l'identità ed i dati di contatto del Titolare del Trattamento, i dati di contatto del responsabile della protezione dei dati, le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento, i legittimi interessi perseguiti dal Titolare del Trattamento o dai terzi, gli eventuali destinatari dei dati personali, ai sensi dell'art. 13 del Regolamento UE 2016/679.

Nel momento in cui i dati personali sono ottenuti, il Titolare fornisce all'Interessato ulteriori informazioni per garantire un trattamento corretto e trasparente quali:

1. l'identità ed i dati di contatto del Titolare del Trattamento;
2. i dati di contatto del responsabile della protezione dei dati;
3. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
4. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
5. ove applicabile, l'intenzione del Titolare del Trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
6. il periodo di conservazione dei dati personali, oppure se non è possibile, i criteri utilizzati per determinare tale periodo;
7. l'esistenza del diritto dell'Interessato di chiedere al titolare l'accesso ai dati personali e la rettifica o la cancellazione degli stessi, ove possibile, o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
8. l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
9. il diritto di proporre reclamo ad un'autorità di controllo;
10. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
11. esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

L'informativa all'Interessato viene fornita per iscritto, anche per estratto, tramite materiale informativo reso disponibile in luoghi comuni del Comune e presso l'apposita sezione del portale web [www.comune.carini.pa.it](http://www.comune.carini.pa.it).

L'informativa sul trattamento dei dati personali non viene rilasciata all'Interessato nel caso in cui questi disponga già delle suindicate informazioni o nel caso in cui comunicarle risulti impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, ricerca storica o a fini statistici, purché in tali casi siano state adottate preventivamente misure tecniche e organizzative adeguate alla protezione dei dati specie al fine di garantire il rispetto del principio della minimizzazione dei dati, e ulteriori misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'Interessato.

Qualora l'Ente intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'Interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Qualora i dati non siano stati ottenuti presso l'Interessato, l'Ente fornisce all'Interessato le seguenti informazioni, ai sensi dell'art. 13 del Regolamento UE 2016/679:

- l'identità e i dati di contatto del Titolare del Trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati, ove applicabile;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- le categorie di dati personali in questione;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'Interessato di chiedere al Titolare del Trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

- qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a) Regolamento UE 2016/679, oppure sull'articolo 9, paragrafo 2, lettera a), Regolamento UE 2016/679 l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, Regolamento UE 2016/679 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

Qualora l'Ente intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'Interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente.

### **Art. 15 - I SOGGETTI COINVOLTI NELLA PROTEZIONE DATI**

Il Regolamento UE 2016/679 ridisegna, in particolare, il ruolo, i compiti e le responsabilità del Titolare, del Responsabile del trattamento dei dati personali e del Responsabile Esterno, in relazione ai nuovi principi e strumenti introdotti dallo stesso, prevedendo delle figure specifiche che ruotano attorno al mondo della protezione dei dati personali:

#### **15.1 - TITOLARE DEL TRATTAMENTO**

Il Comune di Carini, rappresentata ai fini previsti dal Regolamento UE 2016/679 dal Legale Rappresentante pro tempore (Sindaco) è il Titolare del trattamento dei dati personali trattati con strumenti elettronici e cartacei (di seguito indicato con "Titolare"). Il Sindaco può delegare le relative funzioni al personale autorizzato di cui all'art.2- quaterdecies del Codice Privacy.

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 Regolamento UE 2016/679: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento di dati personali è effettuato in modo conforme al Regolamento UE 2016/679. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del Regolamento UE 2016/679, nonché dal Capo III della Parte I del Codice della Privacy.

Il Titolare adotta misure appropriate per fornire all'interessato:

- le informazioni indicate dall'art.13 Regolamento UE 2016/679, qualora i dati personali siano raccolti presso lo stesso interessato;
- le informazioni indicate dall'art.14 Regolamento UE 2016/679, qualora i dati personali non siano stati ottenuti presso lo stesso interessato. Le informazioni saranno rese con le modalità e condizioni previste dagli artt. 77, 78, 79, 80, 82, 89-bis del Codice della privacy.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ed è inserito nel Provvedimento del Garante della Privacy pubblicato in G. U. il 19/11/2018, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art.35 Regolamento UE 2016/679, considerati: la natura, l'oggetto, il contesto e le finalità del medesimo trattamento. La stessa valutazione deve essere fatta nel rispetto dell'art.110 del Codice della privacy, nel caso della ricerca medica, biomedica ed epidemiologica.

Il Titolare, inoltre, nel caso di trattamenti effettuati per suo conto da personale che opera sotto la sua autorità diretta e nell'ambito dell'assetto organizzativo, provvede a designare i suoi Delegati al trattamento a norma del citato art.2-quaterdecies del Codice della Privacy, come previsto dall'Atto aziendale vigente.

I profili di accesso ed i livelli di autorizzazione possono essere differenziati, in conformità all'art. 2-quaterdecies del D.Lgs.196/2003, in modo da assegnare correttamente ruoli ed attività.

I Delegati sono nominati tra il personale del Titolare che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

I delegati sono tenuti a:

- svolgere le attività previste dall'atto di autorizzazione secondo le prescrizioni in esso contenute e le direttive del Titolare/DPO;
- rispettare le norme di sicurezza per la protezione dei dati personali, astenendosi da qualsiasi utilizzo improprio e non necessario del sistema;
- informare il Titolare/DPO in caso di incidente di sicurezza;
- informare il Titolare/DPO in caso di richiesta di accesso da parte di soggetti interessati o autorità giudiziaria.

Ai sensi del medesimo art.2-quaterdecies del Codice Privacy, è consentita la nomina di sub-delegati del trattamento da parte di ciascun Responsabile delegato per specifiche attività di trattamento, nel rispetto degli stessi obblighi che legano il Titolare ed il Responsabile delegato; le operazioni di trattamento possono essere effettuate solo dal personale autorizzato che opera sotto la diretta autorità del Responsabile delegato, attenendosi alle indicazioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Compete al Delegato al Trattamento individuare e nominare, con proprio provvedimento, i subdelegati nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio, che sono tenuti a:

1. conformare la propria azione al pieno rispetto di quanto prescritto dalle leggi vigenti e dalle disposizioni del presente Regolamento.
2. procedere al trattamento attenendosi alle istruzioni impartite dal Titolare del Trattamento il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

I compiti affidati ai subdelegati devono essere analiticamente specificati nell'atto di designazione.

Il Delegato risponde, anche dinanzi al Titolare, dell'operato dei sub-delegati 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-delegato. Il Delegato si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata, l'accesso ai dati trasmessi o comunque trattati.

Il Responsabile 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 o abbia un adeguato obbligo legale di riservatezza.

## **15.2 - RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)**

Il Titolare ha designato il Responsabile della Protezione dei dati (D.P.O.) di cui agli artt.37-39 Regolamento UE 2016/679, il quale redige, custodisce ed aggiorna il Registro delle attività di trattamento, a norma dell'art.30 del Regolamento UE 2016/679; provvede alla notifica all'autorità di controllo in caso di violazione dei dati personali art.33 Regolamento UE 2016/679.

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni

dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il DPO in merito a:

se condurre o meno una DPIA;

1. quale metodologia adottare nel condurre una DPIA;

2. se condurre la DPIA con le risorse interne ovvero esternalizzandola;

3. quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;

4. se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al Regolamento UE 2016/679;

d) cooperare con l'autorità di controllo;

e) può, insieme al Titolare, tenere i registri delle attività di trattamento

f) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

h) dare supporto al Titolare del trattamento alla predisposizione, di concerto con i responsabili dei servizi interessati, della modulistica, delle linee-guida, delle procedure, delle disposizioni operative, e dei registri e policy necessari a rendere operative le indicazioni di legge e del presente documento.

Il Titolare ed il Responsabile del trattamento o Delegato, assicurano che il Responsabile della Protezione dei Dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

- il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il DPO 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 parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tale decisione;
- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Nello svolgimento dei compiti affidatigli il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;
- l'IT Manager o figura equipollente

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti, in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

Fermo restando l'indipendenza nello svolgimento di dette attività, il DPO riferisce direttamente al Titolare o suo delegato o al Responsabile del trattamento. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il Regolamento UE 2016/679 e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare.

Gli Interessati possono contattare il Responsabile della Protezione dei Dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Il Responsabile della Protezione dei Dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

La figura del Responsabile per la protezione dei dati (DPO), può essere ricoperta anche da una figura professionale esterna avente idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati.

### **15.3 - RESPONSABILI ESTERNI**

Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente ai Responsabili esterni del trattamento secondo quanto previsto dall'art.28, Regolamento UE 2016/679, che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate. Questi trattamenti sono disciplinati, a norma dello stesso art.28, par. 3, da un contratto o altro atto giuridico che vincoli il responsabile del trattamento al Titolare. Nel provvedimento di nomina sono analiticamente specificati i compiti affidati al responsabile.

Il contratto o accordo quadro può essere firmato dal Titolare o da un suo delegato. Gli originali sono custoditi dal Titolare o dal delegato, che aggiorna l'elenco dei Responsabili esterni anche per permettere eventuali audit. Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata, l'accesso ai dati trasmessi o comunque trattati. 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 o abbia un adeguato obbligo legale di riservatezza.

Il Responsabile si impegna inoltre ai sensi dell'art. 28, comma 3, lett. F), Regolamento UE 2016/679, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al titolare in relazione agli adempimenti degli obblighi sullo stesso gravanti, di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del Regolamento UE 2016/679 o di comunicazione della stessa agli interessati a norma dell'art. 34 Regolamento UE 2016/679. La comunicazione dovrà avvenire a mezzo PEC all'indirizzo [protocollo@pec.comune.carini.pa.it](mailto:protocollo@pec.comune.carini.pa.it).

Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinnanzi all'Autorità di controllo o all'Autorità Giudiziaria che riguardano il trattamento dei dati di propria competenza. La designazione a Responsabile non comporta alcun diritto per questi ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del contratto principale stipulato con l'Ente.

Per la gestione operativa del sistema, ogni Titolare nomina ed istruisce i soggetti delegati al trattamento. L'incarico è effettuato con atto scritto, nel quale sono analiticamente specificati i compiti affidati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.

#### **Art. 16 - CONTITOLARI DEL TRATTAMENTO**

Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune di Carini da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente e in modo trasparente, mediante accordo interno, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del Regolamento UE 2016/679.

L'accordo definisce le responsabilità di ciascun titolare in merito all'osservanza degli obblighi derivanti dal Regolamento UE 2016/679., con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del Regolamento UE 2016/679, fermo restando eventualmente quanto stabilito dalla normativa europea o statale specificatamente applicabile. Tale accordo può individuare un punto di contatto Provincia per gli interessati.

#### **Art. 17 - AMMINISTRATORE DI SISTEMA**

L'amministratore di sistema nominato dal titolare del Trattamento o da suoi delegati, sovrintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui e' dotato l'Ente. 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 come, 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.

Il Comune applica quanto previsto dal provvedimento del Garante della protezione dei dati personali del 27 novembre 2008, modificato con provvedimento del 25 giugno 2009 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

#### **Art. 18 - PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI (DELEGATI – SUBDELEGATI/AUTORIZZATI)**

Per la gestione operativa del sistema, ogni Titolare del trattamento, nomina ed istruisce i soggetti delegati al trattamento. L'incarico è effettuato con atto scritto, nel quale sono analiticamente specificati i compiti affidati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.

I profili di accesso ed i livelli di autorizzazione possono essere differenziati, in conformità all'Art. 2-quaterdecies del D.Lgs.196/2003, in modo da assegnare correttamente ruoli ed attività.

I Delegati sono nominati tra il personale del Titolare del trattamento che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

Possono essere altresì autorizzati i soggetti che a qualsiasi titolo (ad esempio: tirocinanti, studenti, stagisti, volontari, libero professionisti, borsisti, consulenti, ecc.), prestino la loro opera, anche in via temporanea, all'interno delle strutture dell'Ente e che comportano il trattamento di dati personali.

Tutti i soggetti delegati del trattamento dei dati:

- svolgono le operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento dei dati personali è consentito;
- qualora trattino dati con l'ausilio di strumenti informatici sono personalmente responsabili della gestione riservata della password loro assegnata, ed è fatto loro divieto di cedere la propria password ad altri;
- sono responsabili della custodia riservata dei documenti cartacei loro affidati per effettuare le operazioni di trattamento e hanno l'obbligo di restituirli al termine delle operazioni loro affidate;
- conservano i dati personali su supporto analogico o digitale solo per il tempo previsto dalla normativa vigente per poi successivamente sottoporli a scarto d'archivio o distruzione;
- Devono comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi previsti dagli artt. da 32 a 36 del GDPR;
- Devono fornire al DPO le informazioni utili all'aggiornamento del registro dei trattamenti;
- Non devono permettere il trattamento dei dati personali che, anche a seguito di verifica, risultino eccedenti o non pertinenti o non necessari, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene;
- Devono informare il Titolare/DPO in caso di richiesta di accesso da parte di soggetti interessati o autorità giudiziaria.

Compete al Delegato al Trattamento individuare e nominare, con proprio provvedimento, i subdelegati nel numero ritenuto sufficiente a garantire il corretto funzionamento dell'attività lavorativa, che sono tenuti a:

- a) conformare la propria azione al pieno rispetto di quanto prescritto dalle leggi vigenti e dalle disposizioni del presente Regolamento.
- b) procedere al trattamento attenendosi alle istruzioni impartite dal Titolare del Trattamento il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari;
- c) prendere visione e utilizzare solo i documenti dell'Ente in materia di tutela dei dati personali e del Registro delle Attività di Trattamento vigenti nel tempo relativi alla sua area di riferimento, in base alle funzioni svolte.

I compiti affidati ai subdelegati devono essere analiticamente specificati nell'atto di designazione. Il documento rappresenta un vademecum con le istruzioni operative atte a garantire che il trattamento dei dati personali di cui è Titolare il Comune di Carini e di cui venga a conoscenza il subdelegato al Trattamento durante la sua attività lavorativa, avvenga in conformità a quanto previsto dalla vigente normativa.

## **Art. 19 - ISTRUZIONI DI CARATTERE GENERALE PER TUTTI GLI AUTORIZZATI AL TRATTAMENTO**

Gli Autorizzati al trattamento dei dati devono:

- a) Mantenere il segreto sulle informazioni di cui si venga a conoscenza nello svolgimento della propria attività lavorativa e professionale e nel corso delle operazioni del trattamento, evitando di comunicare le informazioni a terzi. Segreto professionale: tutto il personale del ruolo sanitario, tecnico, professionale e amministrativo, sia del comparto che della dirigenza, e chiunque presti la propria attività lavorativa, anche in veste di consulente, libero professionista o volontario, nei servizi o strutture dell'Ente è tenuto al segreto professionale ossia a non rivelare e/o agevolare in qualsiasi modo, senza giusta causa, la conoscenza delle notizie, dei dati o banche di dati di cui, in ragione e in occasione del proprio stato o ufficio, sia venuto a conoscenza. Si ricorda che

l'eventuale violazione di tale obbligo può comportare l'applicazione di sanzioni di natura deontologica e disciplinare, nonché una responsabilità di natura amministrativa, civile e penale, secondo quanto previsto dal Codice;

- b) fornire l'informativa all'Interessato o alla persona presso cui si raccolgono i dati, con le modalità determinate dall'Autorizzato/Delegato della struttura di appartenenza e utilizzando la modulistica predisposta dall'Ente;
- c) raccogliere, quando richiesto, il consenso dell'Interessato al trattamento dei dati idonei a con le modalità e la modulistica definite dall'Ente;
- d) procedere alla raccolta dei dati personali con la massima cura verificando l'esattezza degli stessi, nonché la pertinenza e la non eccedenza rispetto alle finalità da perseguire;
- e) comunicare i dati personali di natura comune a terzi, solamente se espressamente previsto dalla legge;
- f) comunicare i dati particolari solo a soggetti determinati e, preventivamente e nominativamente, individuati dall'Interessato (con le modalità e la modulistica definite dall'Ente) o solo ove sia espressamente previsto dalla legge;
- g) non diffondere dati idonei a rivelare lo stato di salute. Sarà cura, quindi, dei soggetti che redigono gli atti oggetto di pubblicazione di far sì che si rispetti il divieto considerato. A titolo meramente esemplificativo, si suggerisce la necessità di predisporre la copia degli atti deliberativi da pubblicare, in una forma in cui vi sia il testo della stessa corredato da allegati (questi ultimi, contenenti i dati sanitari, non dovranno essere oggetto di pubblicazione, ma dovranno rimanere agli atti, conservati secondo quanto previsto dalla legge, e a disposizione di coloro che abbiano la legittimazione all'esercizio.

## **Art. 20 - L'INTERESSATO**

L'Interessato (data subject) al [trattamento](#) è la persona fisica cui si riferiscono i [dati personali](#). La normativa attribuisce specifici diritti all'Interessato, il quale, per [l'esercizio di tali diritti](#), può rivolgersi direttamente al [Titolare](#) del. La richiesta deve essere inoltrata all'ufficio Protocollo della Città di Carini, Indirizzo Corso Umberto I, 90044 Carini (PA) o alla mail PEC [protocollo@pec.comune.carini.pa.it](mailto:protocollo@pec.comune.carini.pa.it) l'Interessato può esercitare i suoi diritti anche in un momento successivo a quello in cui ha prestato il [consenso](#), potendo così revocare un consenso già prestato.

I diritti esercitabili dall'interessato sono i seguenti:

- di ottenere informazioni su quali dati sono trattati dal titolare sia se ottenuti presso l'interessato che se non ottenuti presso l'interessato (diritto di informazione);
- di chiedere ed ottenere in forma intellegibile i dati in possesso del titolare (diritto di accesso);
- di revocare il consenso in qualsiasi momento;
- di opporsi al trattamento in tutto o in parte;
- di ottenere la cancellazione dei dati in possesso del titolare (diritto all'oblio), ove possibile;
- di ottenere l'aggiornamento o la rettifica dei dati conferiti;
- di chiedere ed ottenere la trasformazione in forma anonima dei dati;
- di chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento;
- portabilità dei dati.

### **20.1 - DIRITTO DI ACCESSO DELL'INTERESSATO**

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 (art. 15 Regolamento UE 2016/679):

- le finalità del trattamento;
- le categorie di dati personali in questione;
- 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;

- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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;
- il diritto di proporre reclamo al Garante della Privacy;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, 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 relative al trasferimento.

L'Ente fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il Comune di Carini 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.

## **20.2 - 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.

## **20.3 - DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)**

L'Interessato, fatti salvi i casi di esclusione previsti dalla legge, ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.

Il diritto di cancellazione non si applica per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 del GDPR 2016/679.

## **20.4 – DIRITTO DI LIMITAZIONE DEL TRATTAMENTO**

Il diritto di limitazione (art. 18 del regolamento) consente all'Interessato di ottenere il blocco del trattamento nelle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- 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;
- l'interessato si è opposto al trattamento ai sensi dell'art. 21, paragrafo 1 Regolamento (UE) 2016/679, in

attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato. In caso di esercizio di tale diritto ogni trattamento, tranne la conservazione è vietato.

## **20.5 – OBBLIGO DI NOTIFICA IN CASO DI RETTIFICA O CANCELLAZIONE DEI DATI PERSONALI O LIMITAZIONE DEL TRATTAMENTO**

Il Titolare del Trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o 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.

## **20.6 - DIRITTO ALLA PORTABILITÀ DEI DATI**

Nei casi di trattamento effettuato con mezzi automatizzati, l'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano. Nell'esercitare il proprio diritto l'Interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

## **20.7 - DIRITTO DI OPPOSIZIONE**

L'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'Ente si astiene dal trattarli ulteriormente salvo che 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.

Qualora i dati personali siano trattati a fini di ricerca storica o a fini statistici l'Interessato ha il diritto di opporsi al trattamento di dati personali che lo riguardano nel rispetto delle disposizioni previste dal R.E. all'art.89 par. 2 e dal Codice della Privacy 196/2003 come modificato dal D. Lgs 101/2018 art 106 lett. F..

### **Art. 21 - TRATTAMENTI DATI RELATIVI ALL'ATTIVITA' DI WHISTLEBLOWING**

L'istituto del Whistleblowing è stato introdotto in Italia dalla legge 6 novembre 2012, n. 190 (“Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione”) e da ultimo riformato a opera del [decreto legislativo 10 marzo 2023, n. 24](#) che, recependo la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, ha abrogato l'art. 54-bis d.lgs. 165/2001 così come l'art. 3 L. 179/2017, e raccolto in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti sia del settore pubblico che privato. Le disposizioni in esso previste hanno effetto, per i soggetti pubblici, a partire dal 15 luglio 2023.

In tale contesto, il Comune di Carini ha recepito le sopra richiamate novità normative adottando la disciplina organizzativa e procedurale in materia di Whistleblowing.

L'Autorità Nazionale Anticorruzione (ANAC) ha poi provveduto ad adottare, con Delibera n. 311/2023, le “Linee Guida in materia di protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne”, come previsto dall'art. 10 del d.lgs. 24/2023.

Possono essere oggetto di segnalazione violazioni (comportamenti, atti od omissioni) o informazioni sulle violazioni (commesse o che potrebbero essere commesse) di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica e di cui i soggetti segnalanti siano venuti a conoscenza nell'ambito del proprio contesto lavorativo pubblico.

I soggetti nella normativa prima indicata, che vengano a conoscenza nell'ambito del proprio contesto lavorativo all'interno del Comune di Carini, di violazioni o di informazioni sulle violazioni hanno a disposizione diversi canali interni al fine di segnalarle al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) del Comune di Carini:

1. piattaforma informatica disponibile al link <https://www.comune.carini.pa.it/it/page/60699>
2. trasmissione di segnalazione cartacea
3. incontro diretto

La scelta circa il canale da utilizzare è rimessa al soggetto segnalante. Conformemente alla previsione normativa, per ogni canale interno di segnalazione sono state predisposte le opportune misure volte a garantire la riservatezza del segnalante.

In adempimento agli obblighi relativi alla protezione dei dati è pubblicata la seguente informativa: [Informativa whistleblowing](#).

### **Art. 22 - REGISTRO DELLE ATTIVITA' DI TRATTAMENTO**

Il Titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità, costantemente aggiornato, e contiene almeno le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi gli eventuali destinatari di paesi terzi od organizzazioni internazionali;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Ogni responsabile del trattamento tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento.

Entrambi i registri vengono tenuti in forma scritta o anche in formato elettronico e, su richiesta, viene messo a disposizione dell'Autorità Garante della Privacy.

### **Art. 23 - VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA**

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare, prima di procedere al trattamento dei dati personali, effettua una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali consultandosi con il Responsabile della Protezione dei Dati. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi analoghi.

La DPIA è uno strumento importanti 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 sarà condotta in tutti quei casi previsti dal Provvedimento del Garante pubblicato in Gazzetta ufficiale n°269 del 19/11/2018.

La valutazione contiene almeno:

1. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
2. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. una valutazione dei rischi per i diritti e le libertà degli interessati;
4. le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

La decisione in ordine alla possibilità che il trattamento possa produrre un rischio elevato sulla protezione dei dati delle persone fisiche e, quindi, sulla obbligatorietà della DPIA viene adottata applicando i casi indicati l'art. 35, paragrafo 3 del GDPR e i criteri esplicativi contenuti nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida"). Nell'applicare i suddetti criteri si deve tenere conto di quanto segue:

- la DPIA è sempre obbligatoria, indipendentemente dalla presenza di uno o più criteri sopra menzionati, per tutti i trattamenti inclusi nell'elenco predisposto e pubblicato dall'Autorità di controllo ai sensi dell'art. 35, paragrafo 4 GDPR;
- fermo restando che, secondo le Linee guida, un trattamento che soddisfa 2 criteri deve formare oggetto di una valutazione d'impatto sulla protezione dei dati, tuttavia, al fine di garantire una maggiore garanzia di tutela, la ricorrenza anche di 1 solo criterio costituisce elemento sufficiente per originare l'obbligo di svolgimento della DPIA;
- maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati;
- se, pur applicando i criteri sopra indicati, la necessità di una DPIA non emerge con chiarezza, va comunque ritenuto sussistente l'obbligo - secondo quanto raccomandato dal WP29 - di farvi ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento.

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) 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 10 GDPR).

Se necessario l'Ente procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Il Titolare del Trattamento, nello svolgere l'attività di valutazione, si consulta con il Responsabile della protezione dei dati. Laddove la DPIA riveli la presenza di rischi residui elevati, il titolare è tenuto a richiedere la consultazione preventiva dell'Autorità di controllo in relazione al trattamento ai sensi dell' art. 36, paragrafo 1 GDPR.

#### **Art. 24 - VIOLAZIONE DEI DATI PERSONALI – NOTIFICA E COMUNICAZIONE**

Una violazione di dati personali è: *ogni infrazione alla sicurezza degli stessi che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali*

*trasmessi, conservati o comunque trattati dal Titolare del trattamento.*

La violazione di dati è un tipo particolare di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del Regolamento UE 2016/679.

Preliminarmente, dunque, il Titolare deve identificare l'incidente di sicurezza in genere e comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente ci sono dati personali, particolari, giudiziari. Si possono distinguere tre tipi di violazioni:

1. Violazione di riservatezza, quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
2. Violazione di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3. Violazione di disponibilità, quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.
4. In particolari circostanze le violazioni potrebbero essere combinate tra loro.

Il Delegato il Subdelegato e il Responsabile del trattamento sono tenuti ad informare senza ingiustificato ritardo l'Ente del possibile caso di violazione dei dati personali (data breach).

Ogni Interessato può segnalare al Titolare del Trattamento dei dati un possibile caso di violazione dei dati personali. In tali casi il Comune di Carini avvia le necessarie procedure e, avvalendosi della collaborazione del Responsabile del trattamento e del DPO, accerta l'effettivo stato dell'arte.

L'Ente provvede a notificare la violazione all'Autorità Garante della Privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli Interessati. Qualora la notifica non sia effettuata entro 72 ore, questa è corredata dei motivi del ritardo.

La notifica della violazione dei dati personali deve almeno:

- 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;
- comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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.

Il Titolare del Trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio; tale documentazione consente al Garante per la Privacy di verificare il rispetto delle indicazioni di legge.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati a questi viene inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente, salvo i casi di esclusione previsti dalla normativa.

Valutata la necessità di effettuare o meno la notifica della violazione dei dati, l'Ente, procede senza ritardo secondo le modalità stabilite dagli artt.33 e 34 del Regolamento UE 2016/679. Indipendentemente dalla necessità della comunicazione all'Autorità di controllo ed all'Interessato, il Titolare ha predisposto un Registro di Data Breach, tenuto anche dal Responsabile delle Protezione dei dati, contenente:

- il numero della violazione;
- la data della violazione;
- la natura della violazione;
- la categoria degli interessati;

- la categoria dei dati coinvolti;
- le conseguenze della violazione;
- le contro misure adottate;
- la comunicazione o meno al Garante ed all'interessato.

### **Art. 25 - SICUREZZA E CONSERVAZIONE DEI DATI**

Il Comune di Carini adotta misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Tra tali misure vi sono (art. 32 Codice UE):

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

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

- sistemi di autenticazione;
- sistemi di autorizzazione;
- sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio;
- sistemi di rilevazione di intrusione;
- sistemi di protezione con videosorveglianza;
- registrazione accessi;
- porte, armadi e contenitori dotati di serrature e ignifughi;
- sistemi di copiatura e conservazione di archivi elettronici;
- altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

L'Ente assicura inoltre, ai fini di una corretta conservazione, l'adozione di apposite misure e procedure attraverso le quali:

1. si proceda alla distruzione dei dati personali secondo le modalità previste dalla legge e una volta terminato il limite minimo di conservazione, dei documenti analogici e digitali e dei dati personali ivi riportati;
2. siano smaltiti gli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è titolare l'Ente.
3. il riutilizzo di apparati di memoria o hardware sia effettuato con modalità tali da assicurare che non sia possibile accedere ad alcun dato personale di cui è titolare l'Ente.

I responsabili del trattamento sono tenuti ad assicurare al titolare del trattamento di aver adottato, prima di effettuare ogni attività di trattamento dei dati, ogni le misure di sicurezza previste dalla normativa vigente in materia di protezione dei dati e di amministrazione digitale.

L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in

modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

#### **Art. 26 - FORMAZIONE**

L'Ente, nel rispetto dell'art. 32 del GDPR "Sicurezza del trattamento" paragrafo 4 che prevede che "il Titolare del Trattamento ed 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" propone ai propri collaboratori delle sedute formative periodiche per promuovere la cultura della protezione dei dati e per l'aggiornamento informatico giuridico conseguente alle diverse modalità di trattamento. Le attività di formazione possono prevedere anche dei focus mirati su argomenti specifici indirizzati anche a singole unità di personale.

#### **Art. 27 - ATTIVITÀ DI SENSIBILIZZAZIONE**

Il Comune di Carini promuove al suo interno anche attività di sensibilizzazione che possano consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

In tale ottica una delle iniziative di sensibilizzazione sono costituite da attività informative rivolte non solo al personale ma anche coloro che hanno rapporti, a vario titolo con l'Ente.

Oltre a specifiche attività formative finalizzate al continuo aggiornamento del personale autorizzato al trattamento dei dati personali, come previsto dall'art. 34 del presente Regolamento, l'Ente, al fine di garantire la conoscenza capillare delle disposizioni contenute nel Regolamento UE e nel presente documento, ha previsto un'area, all'interno del proprio portale web, accessibile dalla Home Page del sito, dedicata al tema della protezione dei dati personali contenente, oltre al presente documento, la normativa di riferimento, la modulistica da usare nello svolgimento delle attività istituzionali e ogni altra documentazione di supporto.

Inoltre, ad ogni nuova Unità di Personale viene inoltrata una specifica comunicazione con i riferimenti per l'acquisizione e la consultazione del presente Regolamento. Il dipendente, acquisita tale comunicazione, si impegna a scaricarne copia, prendere visione ed attenersi alle prescrizioni dell'Ente in materia di protezione dei dati personali.

#### **Art. 28 - PUBBLICAZIONE GRADUATORIE**

Le graduatorie saranno pubblicate come previsto dal regime di pubblicità delle singole norme di settore ma nel rispetto del principio di pertinenza e non eccedenza. Non possono formare oggetto di pubblicazione: i recapiti degli interessati (utenze di telefonia fissa o mobile, posta elettronica), il codice fiscale, l'indicatore ISEE, il numero di figli disabili, i risultati di test psico attitudinali o i titoli di studio, né quelli concernenti le condizioni di salute degli interessati (ivi compresi i riferimenti a condizioni di invalidità).

#### **Art. 29 - PUBBLICAZIONE ALBO ON LINE**

Salvo diversa disposizione di legge, i documenti da pubblicare sul sito istituzionale per finalità di trasparenza e/o pubblicità non devono consentire l'identificabilità dei soggetti cui i dati si riferiscono quando contengono dati non necessari alla divulgazione, dati di natura particolare, dati giudiziari o di minori. Per quanto sopra, ciascun Ufficio competente alla redazione e conservazione del documento verifica caso per caso, con l'ausilio ove necessario del Responsabile della Protezione dei Dati, e seguendo le istruzioni impartite dalla Direzione Generale, la presenza di eventuali dati da oscurare o rendere anonimi o da pseudonimizzare (quali a titolo esemplificativo ma non esaustivo, numeri telefonici privati, indirizzo di residenza, carta d'identità, patologie, dati del casellario giudiziale, conti correnti bancari etc.), procedendo in tal caso a curare la omissione dei medesimi dati dal contenuto del documento, prima di trasmettere il medesimo per la relativa pubblicazione al soggetto addetto a tale attività.

### **Art. 30 - IL DIRITTO DI ACCESSO E IL DIRITTO ALLA RISERVATEZZA**

Il Comune di Carini, in osservanza delle disposizioni vigenti in materia di riservatezza e trasparenza, valuta, anche con riguardo ad altre regolamentazioni specifiche, caso per caso la possibilità da parte di terzi di accedere a documenti contenenti dati personali e particolari. L'accesso ai dati idonei a rivelare lo stato di salute o la vita sessuale o l'orientamento sessuale di un terzo (art. 60 Codice Privacy) è ammesso solo quando il diritto da tutelare, tramite istanza di accesso, è di rango almeno pari al diritto alla riservatezza, ovvero consiste in un diritto della personalità o altro diritto o libertà fondamentale ed inviolabile, quale ad esempio il diritto alla difesa, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso.

Fatto salvo quanto sopra, i presupposti, le modalità, i limiti per il diritto di accesso a documenti amministrativi contenenti dati personali e la relativa tutela giurisdizionale, restano disciplinati dalla Legge 7/8/1990, n. 241 ed s.m.i. e dalle altre disposizioni di legge in materia.

I presupposti, le modalità ed i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal Decreto Lgs 14 marzo 2013, n.33, come modificato dal D. lgs n.97/2016 e s.m.i..

### **Art. 31 - PUBBLICAZIONE NELL'AMMINISTRAZIONE TRASPARENTE**

Salvo diversa disposizione di legge, i documenti da pubblicare sul sito istituzionale per finalità di trasparenza e/o pubblicità non devono consentire l'identificabilità dei soggetti cui i dati si riferiscono quando contengono dati non necessari alla divulgazione, dati di natura particolare, dati giudiziari o di minori.

Per quanto sopra, ciascun Ufficio competente alla redazione e conservazione del documento verifica caso per caso, con l'ausilio ove necessario del Responsabile della Protezione dei Dati, e seguendo le istruzioni impartite dalla Direzione Generale, la presenza di eventuali dati da oscurare o rendere anonimi o da pseudonimizzare (quali a titolo esemplificativo ma non esaustivo, numeri telefonici private, indirizzo di residenza, carta d'identità, patologie, dati del casellario giudiziale), procedendo in tal caso a curare la omissione dei medesimi dati dal contenuto del documento, prima di trasmettere il medesimo per la relativa pubblicazione al soggetto addetto a tale attività.

### **Art. 32 - UTILIZZO HARDWARE E SOFTWARE**

Il Personal Computer o il pc portatile affidati al dipendente sono uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può determinare un livello di sicurezza non adeguato oltre a disservizi e costi di manutenzione.

L'Ufficio informatico potrà accedere ai dati e agli strumenti informatici esclusivamente per permettere al Titolare del Trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dall'Ente, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività lavorativa nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo autorizzazione esplicita del Responsabile dei sistemi informatici dell'Ente, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Responsabile dei sistemi informatici.

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre il Comune di Carini a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del Responsabile dei sistemi informatici.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate

dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del Responsabile dei sistemi informatici.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile dei sistemi informatici nel caso in cui vengano rilevati virus.

### **Art. 33 - UTILIZZO DELLA RETE**

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le indicazioni impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

Il Responsabile dei sistemi informatici può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati.

E' infatti assolutamente da evitare un'archiviazione ridondante.

### **Art. 34 - RILASCIO CREDENZIALI DI AUTENTICAZIONE**

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal Responsabile dei sistemi informatici.

E' necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al Responsabile dei sistemi informatici.

La password deve essere immediatamente sostituita, dandone comunicazione al Responsabile dei sistemi informatici, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a dare immediata notizia alla Direzione o al Responsabile dei sistemi informatici.

### **Art. 35 - USO DELLA POSTA ELETTRONICA DELLA RETE INTERNET E DEI RELATIVI SERVIZI**

La casella di posta assegnata dal Comune di Carini all'utente ed il PC abilitato alla navigazione in Internet sono strumenti di lavoro, ogni utilizzo non inerente all'attività lavorativa può determinare un livello di sicurezza non adeguato oltre a disservizi e costi di manutenzione. Le persone assegnatarie delle caselle di posta elettronica e della rete internet sono responsabili del corretto utilizzo delle stesse. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

La posta elettronica è uno strumento messo a disposizione esclusivamente per motivi di lavoro a tutti i dipendenti (e collaboratori) al momento della loro contrattualizzazione; di conseguenza deve essere utilizzato in tale ambito, nel rispetto degli obblighi derivanti dalle norme di legge e dalle clausole contrattuali che disciplinano il rapporto di lavoro.

Gli Utenti, assegnatari delle caselle di posta elettronica, sono responsabili del corretto utilizzo delle stesse e devono mantenerle in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Si raccomanda di

cancellare periodicamente le mail ricevute e inviate non necessarie e svuotare il cestino con le mail eliminate. L'Utente che si assenta per lunghi periodi (ferie) deve provvedere ad attivare l'opzione "Assente o Fuori sede" in cui indicare chi contattare in sua assenza.

In caso di cessazione del rapporto di lavoro o di collaborazione, la casella di posta elettronica individuale sarà disattivata immediatamente (a tale scopo, risulta obbligatorio comunicare la fine del rapporto lavorativo).

È onere del dipendente assegnatario della casella di posta un attento monitoraggio della stessa in quanto le comunicazioni via mail assumono formale carattere istituzionale.

È vietato utilizzare indirizzi e-mail non istituzionali per trasmettere messaggi connessi alla propria attività istituzionale.

#### **Art. 36 - RESPONSABILITÀ IN CASO DI VIOLAZIONE DELLE DISPOSIZIONI IN MATERIA DI PRIVACY**

Il mancato rispetto delle disposizioni in materia di protezione dei dati personali è punito con le sanzioni di natura amministrativa e di natura penale previste dagli art. da 166 a 172 del D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018 nonché con sanzioni di natura disciplinare per violazione di regolamenti del Comune di Carini.

Il Responsabile del trattamento risponde per danno causato dal trattamento se non ha adempiuto agli obblighi previsti dal presente Regolamento a lui specificatamente attribuiti o ha agito in modo difforme o contrario rispetto alle istruzioni impartite 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 a loro imputabile.

#### **Art. 37 - RINVIO A DISPOSIZIONI DI LEGGE**

Per quanto non espressamente previsto nel presente regolamento, si fa rinvio al Regolamento Europeo 2016/679 del 27/4/2016 ed al D. Lgs. n.196/03, modificato dal D. Lgs. n.101/2018, ai provvedimenti specifici del Garante per la protezione dei dati personali ed alle disposizioni normative correlate.