COMUNE DI ORISTANO

Comuni de Aristanis

Regolamento sulla protezione dei dati personali

in attuazione del Regolamento (UE) N° 2016/679

Approvato con deliberazione C.C. n. …….. in data …….

Sommario

CAPO I - DISPOSIZIONI GENERALI

Art. 1
Quadro normativo di riferimento

Il presente Regolamento tiene conto dei seguenti documenti:

- Codice in materia di dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016 (D.Lgs. n.196/2003, come modificato dal D.Lgs 101/2018);
- Linee guida e raccomandazioni del Garante;
- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- D.Lgs. n. 101/2018 di adeguamento della normativa interna al GDPR;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento"possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalita' - 13/EN WP 203;
- Allegato 1 al provvedimento n. 467 del 11 ottobre 2018 "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto";
- Norme internazionali;
- Regolamenti interni, approvati dai titolari e/o dai responsabili.

Art. 2
Definizioni

Il presente regolamento si avvale delle seguenti definizioni:

- **"Codice"**: D.Lgs. n. 196/2003, come modificato dal D.Lgs 101/2018;
- **"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);

- **Garante della Privacy:** l'Autorità di controllo**;**
- **"Regolamento":** il presente Regolamento;
- "**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;
- **"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;
- **"limitazione di trattamento":** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **"profilazione":** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **"pseudonimizzazione":** il trattamento dei dati personali in modo tale che gli stessi 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;
- **"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;
- **"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. Ai fini del presente regolamento il Titolare del Trattamento è il Comune di Oristano nella persona del Sindaco Pro Tempore;
- **"Contitolari del trattamento":** due o più titolari del trattamento che determinano congiuntamente, mediante accordo interno, le finalità e i mezzi del trattamento;
- **"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;
- **"Delegato al trattamento":** la persona fisica legata al Comune di Oristano da un rapporto di Lavoro e attribuzione di qualifica dirigenziale o di posizione organizzativa, che esercita i poteri delegati dal Titolare o che è nominato dal Titolare per esercitare tali poteri.
- "Incaricato del trattamento": la persona fisica legata al Comune di Oristano da un rapporto di lavoro, nominato dal Dirigente/PO, che agendo sotto l'autorità del Titolare/delegato al trattamento, abbia accesso ai dati personali essendo stato autorizzato al loro trattamento;
- **"Responsabile della Protezione dei dati" (RPD):** la persona fisica o giuridica che svolge i compiti di

cui all'art. 39 del REG.UE 2016/679 e/o ulteriori compiti affidati dal Titolare del trattamento, anche sulla base di un contratto di servizi;

- **"Amministratore di sistema:** la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché all'amministrazione di basi di dati, di reti e di apparati di sicurezza e di sistemi software complessi;
- **"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;
- **"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;
- **"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;
- **"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;
- **"dati genetici":** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **"dati biometrici":** 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;
- **"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;
- **"stabilimento principale":**
    a) per quanto riguarda un Titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua Amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
    b) con riferimento a un Responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua Amministrazione centrale nell'Unione o, se il Responsabile del trattamento non ha un' Amministrazione centrale nell'Unione, lo stabilimento del Responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del Responsabile del trattamento nella misura in cui tale Responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
- **"rappresentante":** la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- **"impresa":** la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti

un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

- **"gruppo imprenditoriale":** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- **"norme vincolanti d'impresa":** le politiche in materia di protezione dei dati personali applicate da un Titolare del trattamento o Responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un Titolare del trattamento o Responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- **"autorità di controllo interessata":** un'autorità di controllo interessata dal trattamento di dati personali in quanto:
  - il Titolare del trattamento o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
  - gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
    oppure
  - un reclamo è stato proposto a tale autorità di controllo;
- **"trattamento transfrontaliero":**
  - trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del trattamento o Responsabile del trattamento nell'Unione ove il Titolare del trattamento o il Responsabile del trattamento siano stabiliti in più di uno Stato membro;
    oppure
  - trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare del trattamento o Responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- **"obiezione pertinente e motivata":** un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del GDPR, oppure che l'azione prevista in relazione al Titolare del trattamento o Responsabile del trattamento sia conforme al GDPR, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertaà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
- **"servizio della società dell'informazione":** il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- **"organizzazione internazionale":** un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art. 3
Oggetto

Il presente Regolamento disciplina le misure procedimentali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo n. 679 del 27 aprile 2016 "Regolamento generale sulla protezione dei dati" (RGPD) e attuato con D. Lgs n°101/2018.
Esso ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali nonché alla libera circolazione di tali dati effettuato dal Titolare, nel rispetto di quanto previsto dal RGPD e sostituisce integralmente il precedente Regolamento sulla privacy, approvato con deliberazione C.C. n. 11 in data 24/01/2006.

Art. 4
Finalità

Il Comune di Oristano effettua i trattamenti dei dati personali per finalità di pubblico interesse stabilite dalle fonti normative che ne regolano le funzioni e in particolare:

1. l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nel cui ambito i trattamenti sono compiuti per:
    a) 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;
    b) la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
    c) l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale o regionale o provinciale trasferite o delegate o comunque affidate al Comune in base alla vigente legislazione.
    d) l'adempimento di un obbligo legale al quale è soggetto il Comune;
    e) l'esecuzione di un contratto con riguardo ai soggetti interessati;
    f) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Il Comune di Oristano 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. Garantisce inoltre, nell'ambito delle sue funzioni, la gestione degli archivi e delle banche dati nel rispetto dei diritti, delle libertà fondamentali e della 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 Comune di Oristano sono gestiti conformemente alle disposizioni del Codice, del GDPR, e del presente Regolamento.

CAPO II - PRINCIPI

Art. 5
Principi e responsabilizzazione

I dati personali sono trattati nel rispetto dei principi dettati dal GDPR, e qui integralmente recepiti, tali principi sono di:

a) «**liceità, correttezza e trasparenza**»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) «**limitazione delle finalità**»: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ;

c) «**minimizzazione dei dati**»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) «**esattezza**»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) «**limitazione della conservazione**»: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, prf. 1 del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;

f) «**integrità e riservatezza**»: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, verso trattamenti non autorizzati o illeciti e verso la perdita, la distruzione o i danni accidentali.

g) «**responsabilizzazione**»: il Titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di comprovarlo.

Nelle ipotesi in cui disposizioni legislative, regolamentari o statutarie prevedano pubblicazioni obbligatorie, il responsabile del procedimento adotta le opportune misure atte a garantire la riservatezza dei dati personali a norma del RGPD, del "Codice della privacy" di cui al d.lgs. 30 giugno 2003.n. 196, del "Codice della trasparenza" di cui al d.lgs. 14 marzo 2013, n. 33 e dei provvedimenti del Garante della Privacy

Art. 6
Liceità del trattamento

Il trattamento dei dati personali effettuato da questo Comune 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.

f) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) non si applica al trattamento di dati effettuato dal Titolare nell'esecuzione dei propri compiti e funzioni.

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 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
Condizioni per il consenso

Il Comune di Oristano non richiede agli interessati il consenso per il trattamento dei loro dati personali allorquando il trattamento dei dati è effettuato nello svolgimento dei propri compiti istituzionali di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito dal diritto dell'Unione o dello Stato, ed in particolare per quelli ricompresi nelle lettere da a) ad e) dell'articolo 4 del presente regolamento.

Nei casi in cui il trattamento dei dati personali, per una o più specifiche finalità, è subordinato al consenso dell'interessato si prevede 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 e 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.
5) per i dati sensibili il consenso deve essere esplicito e in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;
6) il consenso dei minori è valido a partire dai 16 anni, fermo restando il diverso limite di età, comunque non inferiore a 13 anni, previsto dalla normativa nazionale; prima del limite di età previsto dalla normativa

nazionale occorre raccogliere il consenso dei genitori o di chi ne fa le veci;

7) deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto attraverso ad es. caselle prespuntate su un modulo;
8) deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

Se il consenso dell'interessato al trattamento dei propri dati personali 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 GDPR e del presente Regolamento, è vincolante.

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.

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

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

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

Il consenso viene registrato nel registro delle attività di trattamento.

Art. 8
Informativa

Il Comune di Oristano, al momento della raccolta dei dati personali, fornisce all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dal GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

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

L'informativa è fornita, mediante idonei strumenti:

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

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

Qualora il Titolare del trattamento 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.

Art. 8 bis
Contenuto dell'Informativa

L'informativa contiene il seguente contenuto minimo:

a) l'identità e dati di contatto del Titolare del trattamento quale Comune di Oristano con il suo rappresentate legale/sindaco pro tempore;
b) i dati di contatto del Responsabile della protezione di dati (RPD/DPO) esterno all'Ente;
c) le finalità del trattamento;
d) i destinatari dei dati;
e) la base giuridica del trattamento;
f) l'interesse legittimo del Titolare se quest'ultimo costituisce la base giuridica del trattamento;
g) se il Titolare trasferisce i dati personali in Paesi terzi, deve indicare attraverso quali strumenti;

In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il Comune fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente

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

Art. 8 ter
Informativa per dati raccolti presso soggetti diversi dall'interessato

Nel caso di dati personali non raccolti direttamente presso l'interessato, oltre alle informazioni indicati all'articolo precedente:

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

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

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

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

Apposite informative devono essere inserite nei seguenti documenti:

1. nei bandi e nella documentazione di affidamento dei contratti pubblici,
2. nei contratti, accordi o convenzioni,
3. nei bandi di concorso pubblico,
4. nelle segnalazioni di disservizio,
5. in ogni altro documento contenente dati personali.

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

Art. 9
Sensibilizzazione e formazione

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.
A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del Titolare e l'attività informativa diretta a tutti coloro che hanno rapporti con il Titolare.
Per garantire la conoscenza capillare delle disposizioni del presente Regolamento, al momento dell'ingresso in servizio è data a ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale, con i riferimenti per l'acquisizione del presente Regolamento, pubblicato sul sito del Titolare.
Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.
Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.
La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata, a cura del RPC, con la formazione in materia di prevenzione della corruzione e della illegalità nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Titolare.
La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale

CAPO III - IL TRATTAMENTO DEI DATI PERSONALI

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

Il Titolare, tratta i dati personali per lo svolgimento dei propri fini istituzionali, come stabilite da disposizioni di legge, statuti e regolamenti, e nei limiti imposti dal Codice, dal GDPR e dalle Linee guida, nonché ~~e~~ dai provvedimenti del Garante.

I trattamenti di dati personali riguardano a titolo esemplificativo e non esaustivo:

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

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

1) Titolare
2) dirigenti/P.O., in qualità di soggetti che esercitano i poteri delegati dal Titolare o in qualità di soggetti nominati dal Titolare per l'esercizio di tali poteri
3) dipendenti, in qualità di incaricati del trattamento.

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

Ai fini del trattamento, il Titolare provvede, in collaborazione con i dirigenti/P.O., all'integrale ricognizione ed aggiornamento di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti del Titolare medesimo, funzionali alla formazione dell'indice dei trattamenti.

È compito dei dirigenti/P.O. effettuare e documentare l'aggiornamento periodico, almeno annuale, della ricognizione dei trattamenti e del relativo indice, e la valutazione periodica, del rispetto dei principi di cui all'articolo 5 del presente Regolamento con riferimento a tutti trattamenti inclusi nell'indice.

Art.11
Tipologie di dati trattati

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

a) dati comuni identificativi.
b) dati sensibili.
c) dati giudiziari.

Art. 12
Trattamento di particolari categorie di dati (sensibili)

Il Comune di Oristano si conforma all'articolo 2-*septies* del Codice nonché alle Linee Guida del Garante in materia di trattamento dei dati personali sensibili relativi allo stato di salute.

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

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

Art.13
Trattamento dei dati giudiziari

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

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 del RGPD deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il

trattamento è autorizzato dal diritto dell'Unione o dello Stato deve prevedere garanzie appropriate per i diritti e le libertà degli interessati.
A tale fine, applica i principi degli articoli 9 paragrafo 1 del GDPR e l'articolo 2-*sexies* del Codice e si conforma alle Linee Guida del Garante in materia, e sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati giudiziari.

Art. 14
Trattamento dei dati del personale

Il Titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo.
Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.
Secondo la normativa vigente, il Titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica.
Il trattamento dei dati sensibili del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo dei dati giudiziari e sensibili, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.
La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici.
Non sono infatti ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.
Il Titolare, nel trattamento dei dati sensibili relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità, e si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 15
Registro delle attività di trattamento e delle categorie di trattamento

Il Titolare del trattamento ha istituito un registro, in forma scritta, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità.
Il registro viene continuamente aggiornato e messo a disposizione delle autorità di controllo.
Tale registro conforme all'art.30 del GDPR, contiene le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento, del Responsabile per la protezione dei dati, dei dirigenti/delegati e degli incaricati/uffici interessati;
b) le finalità del trattamento;
c) le categorie di interessati;

d) le categorie dei dati personali;
e) le categorie dei trattamenti effettuati;
f) le categorie di destinatari, a cui i dati personali sono o saranno comunicati;
g) un'eventuale possibilità di trasferimenti di dati all'estero;
h) indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

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

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del Titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 GDPR.

I registri sono tenuti in forma scritta, anche in formato elettronico.

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

Art. 16
Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

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

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

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

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

In ogni caso, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere sensibile o giudiziario dell'interessato, devono essere anonimizzati con adeguate tecniche di anonimizzazione.

I dati sensibili e giudiziari sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.

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

CAPO IV - I DIRITTI DEGLI INTERESSATI

Art. 17
Diritti dell'interessato

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

Art. 18
Diritto di accesso

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

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.
Il Titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.
Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.
I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati sensibili e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.
Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
Il Titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

Art. 19
Diritto alla rettifica e cancellazione

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di rettifica e cancellazione ("diritto all'oblio"), di seguito indicata.
Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
Il Titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
Quanto al diritto "all'oblio", consistente nel diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:

1. per l'esercizio del diritto alla libertà di espressione e di informazione;
2. per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
3. 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 GDPR;
4. a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
5. per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 20
Diritto alla limitazione

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto alla limitazione di seguito indicata.
L'interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:

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

Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 GDPR, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal Titolare prima che detta limitazione sia revocata.

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

Art. 21
Diritto alla portabilità dei dati

Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, il diritto alla portabilità dei dati non si applica al trattamento 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.

Art. 22
Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione sulla base di tali disposizioni.
Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il diritto di opposizione di cui ai paragrafi 1 e 2 dell'art. 21 GDPR è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del GDPR, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Art. 23
Modalità di esercizio dei diritti dell'interessato

Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR, del Codice e del presente Regolamento.
La richiesta per l'esercizio dei diritti può essere fatta pervenire:

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

giuridica, un ente o un'associazione.

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

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

La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.

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

Soggetto competente alla valutazione dell'istanza è il dirigente/P.O competente, il quale decide sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.

All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa.

I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.

L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del Titolare; l'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.

Il Comune di Oristano si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Art. 24
Indagini difensive

Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'articolo 391-*quater* del Codice di procedura penale, può chiedere documenti in possesso del Titolare, e può estrarne copia, anche se contengono dati personali di un terzo interessato.

Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile rinviando, per ogni altro e ulteriore aspetto, alla relativa disciplina e al Regolamento del Titolare sul diritto di accesso.

Il Titolare si conforma alle Linee guida del Garante in tema di indagini difensive.

CAPO V - SOGGETTI

Art. 25
Titolare e contitolari

Il Titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee, gestite dagli uffici comunali, è il Comune di Oristano, rappresentato dal Sindaco pro tempore, in qualità di legale rappresentante del Titolare, con sede in Piazza Eleonora n. 44, 09170 Oristano.

Il Titolare provvede:

a) a definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento, provvedendo all'inserimento di tali obiettivi strategici nel DUP e negli altri documenti di programmazione e pianificazione del Titolare;
b) a designare, con proprio atto, il Responsabile per la protezione dei dati personali;
c) nominare l'Amministratore del Sistema informatico;

d) a delegare ovvero a nominare, con proprio atto, i dirigenti/P.O. per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti, e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi, le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
e) a formare e aggiornare l'elenco dei dirigenti/P.O., delegati o nominati, e a pubblicarlo sul sito web istituzionale del Titolare;
f) a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Codice, al GDPR e al presente Regolamento;
g) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
h) a favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
i) a favorire l'adesione a meccanismi di certificazione;
j) ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa;

Il Titolare si trova in rapporto di contitolarità con altri titolari quando determinano congiuntamente le finalità e i mezzi del trattamento, secondo quanto previsto dall'art. 26 GDPR.
I contitolari sono tenuti a determinare, in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR e dal presente Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, fermo restando eventualmente quanto stabilito dalla normativa europea o statale cui i titolari del trattamento sono soggetti. Tale accordo può determinare un punto di contatto per gli interessati. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
Indipendentemente dalle disposizioni dell'accordo interno, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun Titolare del trattamento.

Art. 26
Delegati dal Titolare

Il Titolare nella persona del Sindaco designa i responsabili interni del trattamento quali delegati individuati nelle persone dei dirigenti /P.O. e conferisce loro i sotto indicati compiti e funzioni, e i correlati poteri, mediante apposito provvedimento di delega o di nomina, col quale informa ciascuno di essi delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento, compiti, funzioni e poteri:

a) trattare i dati personali solo su istruzione del Titolare del trattamento;
b) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adottare il tempestivo ed integrale rispetto dei doveri del Titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del GDPR;
d) osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal Titolare;
e) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che

comunque incidono sul trattamento dei dati;

f) collaborare con il Titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in collaborazione con l'amministratore di sistema e con le altre strutture competenti del Titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
g) curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del Titolare per l'applicazione del Codice, del GDPR, e del presente Regolamento;
h) assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;
j) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, GDPR e nel presente Regolamento;
k) contribuire alle attività di verifica del rispetto del Codice, del GDPR e del presente regolamento, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato;
l) curare la costituzione e l'aggiornamento dei seguenti archivi/banche dati, per quanto di competenza:
    1. elenco dei contitolari, dei responsabili dei trattamenti, e degli incaricati, con i relativi punti di contatto;
    2. elenco degli archivi/ banche;
m) garantire l'aggiornamento, almeno annuale, della ricognizione dei trattamenti;
n) fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

Ciascun dirigente/P.O., nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, collabora con il Titolare al fine di:

1) comunicare tempestivamente, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato; la redazione della valutazione d'impatto sulla protezione dei dati; la consultazione preventiva;
2) predisporre le informative previste e verificarne il rispetto e fornire le informazioni necessarie per l'aggiornamento del registro dei trattamenti;
3) designare gli incaricati del trattamento, e fornire loro specifiche istruzioni;
4) rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
5) garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della struttura organizzativa del Titolare ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali responsabili del trattamento;
6) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

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

I dirigenti/P.O. sono destinatari degli interventi di formazione di aggiornamento.

Art. 27
Responsabili del trattamento e sub responsabili

Il Responsabile del trattamento è il soggetto pubblico o privato esterno all'Ente che agisce per conto del Titolare sulla base di un affidamento di lavori, servizi o forniture tramite delega, concessione o contratto, di competenza di questo Comune da cui ne consegue il trattamento di dati personali. Il provvedimento o contratto di responsabilità deve prevedere norme specifiche attraverso le quali si provvede:

a) ad impartire compiti e responsabilità in ordine al trattamento e alla protezione dei dati personali che dovranno trattare per conto del Titolare per la durata dell'affidamento;
b) ad obbligare il soggetto affidatario ad osservare le prescrizioni di cui al RGPD e alle altre fonti di diritto dell'Unione e dello Stato in materia di protezione dei dati personali;
c) a consentire le verifiche sul rispetto delle predette disposizioni normative.

Nell' ipotesi di trattamento dei dati personali di cui al precedente comma, il Delegato competente per materia in relazione al compito e/o al servizio affidato, ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; e l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.

La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, é determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento.

Il Responsabile è designato dal Titolare per il tramite del Dirigente delegato, competente per materia che ha affidato l'incarico e/o il servizio attraverso la predisposizione entro 20 gg dalla firma del contratto di servizio/lavoro/incarico, di apposito contratto che lo autorizzi a trattare i dati personali per conto del Titolare.

I responsabili del trattamento, forniscono le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale da parte del Titolare.

Il Titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali, verificherà che i Responsabili del trattamento dei dati personali, presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Per specifiche attività di trattamento è consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento. Le operazioni di trattamento possono essere effettuate solo da incaricati che operino sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuino specificatamente l'ambito del trattamento consentito.

Il Responsabile risponde dinanzi al Titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sul suo operato.

I Responsabili del trattamento hanno l'obbligo di:

1) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia;
2) rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
3) nominare al loro interno i soggetti incaricati del trattamento;

4) garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento;
5) trattare i dati personali, anche di natura sensibile e sanitaria esclusivamente per le finalità previste dal contratto o dalla convenzione;
6) attenersi alle disposizioni impartite dal Titolare del trattamento;
7) specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti;
8) comunicare le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

Nel caso di mancato rispetto delle predette disposizioni, e in caso di mancata comunicazione al Titolare dell'atto di nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso il Titolare, il Responsabile del trattamento.
La designazione del Responsabile viene effettuata mediante atto da parte del Titolare del trattamento da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente al Titolare.
L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Art. 28
Incaricati del trattamento dipendenti del Titolare

Gli incaricati del trattamento sono le persone fisiche, dipendenti del Titolare, designati da ciascun dirigente. Sono figure di primissima rilevanza nell'organigramma dell'Ente ai fini della privacy poiché, sotto la diretta autorità del Titolare e dei delegati, sono incaricati, dietro apposita nomina ad effettuare materialmente le operazioni di trattamento sui dati personali di propria competenza, con l'indicazione specifica dei compiti, dell'ambito di trattamento consentito, delle modalità nell'ambito dei procedimenti assegnati.
La designazione dell'incaricato al trattamento dei dati personali è di competenza del dirigente/P.O., la nomina è effettuata per iscritto e individua specificatamente i compiti spettanti all'incaricato e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.
I dipendenti comunali sono designati Incaricati e autorizzati al trattamento dei dati personali con formale provvedimento del Dirigente delegato del Titolare, competente per la struttura organizzativa apicale in cui sono inseriti gli stessi dipendenti. Nel provvedimento sono indicati i procedimenti amministrativi per lo svolgimento dei quali è indispensabile il trattamento dei dati personali, le finalità del trattamento, le categorie di dati personali da trattare, le operazioni di trattamento eseguibili, gli eventuali limiti al trattamento, le misure di sicurezza da adottare da parte degli stessi Incaricati.
Le predette designazioni e autorizzazioni nonché le prefate indicazioni del trattamento sono stabilite con un atto distinto dal contratto individuale di lavoro. Tale atto deve essere notificato al dipendente interessato, il quale non può esimersi dalla sua accettazione e attuazione.
Gli incaricati collaborano con il Titolare ed il dirigente/P.O. segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.
In particolare, gli incaricati devono assicurare che, nel corso del trattamento, i dati siano:

1. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
3. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
5. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;

6. trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

Gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal dirigente/P.O., nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del Titolare.

Nel caso di allontanamento anche temporaneo dalla propria postazione di lavoro, l'incaricato verifica che non vi sia possibilità per chiunque non sia autorizzato all'accesso ai dati di accedere alle banche-dati e/o ai dati personali per i quali è in corso un qualsiasi tipo di trattamento.

Gli incaricati dipendenti del Titolare sono destinatari degli interventi di formazione e di aggiornamento.

Art. 29
Incaricati del trattamento non dipendenti del Titolare

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

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

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

Art. 30
Amministratore di sistema

Al fine di ottemperare a quanto disposto dal Garante della Privacy il Comune si avvale obbligatoriamente di un amministratore del sistema informatico, individuato nel Responsabile del Centro Elaborazione Dati, al fine di assicurare che il sistema informatico dell'Ente sia strutturato e gestito in modo da garantire le misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema.

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. Può essere designato un dipendente comunale a tempo indeterminato inquadrato almeno nella categoria "D", ovvero, nel caso di mancanza di un dipendente, un soggetto esterno, persona fisica o soggetto giuridico. La designazione dell'amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

L'amministratore di sistema svolge attività, quali:

1) 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;
2) verificare costantemente che il Titolare del trattamento adotti le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, provvedendo nel caso agli adeguamenti eventualmente necessari;
3) proporre al Titolare del trattamento e ai Delegati l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati atte a che i dati personali oggetto di trattamento siano

custoditi e controllati , anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stesi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici.

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

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

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

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

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

Il Responsabile della protezione dei dati procede, alla verifica delle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Art. 31
Responsabile della protezione dei dati personali (RPD)

Il Comune si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD), in possesso delle qualità professionali, in particolare di un'adeguata conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali e della capacità di adempiere alle funzioni in totale indipendenza e in assenza di conflitti di interesse.

Il Responsabile della protezione è designato con decreto del Sindaco quale rappresentante legale pro tempore del Titolare del trattamento dei dati Comune di Oristano.

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

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

Il RPD svolge i seguenti compiti:

1) informa e fornisce consulenze al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
2) verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
3) sorveglia sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dai suoi delegati e incaricati;
4) fornisce, qualora venga richiesto, pareri in merito a qualunque dubbio, incertezza o incongruenza sorga in merito al trattamento dei dati, agli atti da emettere, ad eventuali perdite di dati o misure da applicare e anche in ordine alla valutazione d'impatto sulla protezione dei dati (DPIA) e ne sorveglia lo svolgimento ai sensi dell'art. 35 del RGPD; il Titolare del trattamento per il tramite del referente dell'Ente, in particolare, si consulta con il RPD in merito a:
    a) se condurre o meno una DPIA;

b) quale metodologia adottare nel condurre una DPIA;
c) se condurre la DPIA con le risorse interne ovvero esternalizzandola;
d) quali salvaguardie applicare, comprese misure tecniche ed organizzative, per attenuare i rischi delle persone interessate;
e) 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 RGPD;

5) verifica e predispone referto annuale, riguardo alle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
6) funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
7) coopera con il Garante per la protezione dei dati personali e funge da punto di contatto per detta Autorità per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva di cui all'art. 36 del RGPD, ed effettua, se del caso, consultazioni relativamente a ogni altra questione.

Il Titolare e i delegati del trattamento si assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Art. 32
Referente privacy dell'Ente.

Il Sindaco nomina con proprio Decreto un dipendente di categoria D quale referente dell'Ente che collabori con il Responsabile per la protezione dei dati personali (RPD), tenga i contatti con i delegati e gli incaricati del trattamento dei dati personali e si occupi delle comunicazioni ad Enti Terzi previste dal GDPR e dal Garante della privacy.

Art. 33

Comunicazione interna di documenti contenenti dati personali

La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lettera a) del DPR n. 445/2000, contenenti dati personali ai componenti degli organi di governo ovvero all'interno della struttura organizzativa di questo Comune, per ragioni d'ufficio e nell'ambito delle specifiche competenze dei servizi, non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti.
Il Responsabile del trattamento può tuttavia disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione concerna dati sensibili e/o giudiziari.

Art. 34

Utilizzo di dati da parte degli organi di governo e di controllo interno

Il Sindaco, i Consiglieri comunali e gli Assessori nonché i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti da questo Comune contenenti dati personali nei limiti e con le modalità previsti dalle disposizioni di legge e di regolamenti.
Le notizie e le informazioni così acquisite devono essere utilizzate esclusivamente per le finalità pertinenti alle rispettive competenze, rispettando il divieto di divulgazione dei predetti documenti nonché l'obbligo della

segretezza del loro contenuto

CAPO VI - SICUREZZA DEI DATI PERSONALI

Art. 35
Misure di sicurezza

Il Titolare, i delegati, l'Amministratore del sistema informatico e il Responsabile della protezione dei dati personali, garantiscono per quanto di competenza l'adozione e l'applicazione di adeguate misure di sicurezza che consentano di ridurre al minimo i rischi di distruzione, perdita (anche accidentale), di accesso non autorizzato, di trattamento non consentito o non conforme alla finalità della raccolta dei dati stessi, secondo quanto previsto dal Piano di protezione dei dati personali adottato dall'ente.
Il Titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate per garantire un livello di sicurezza adeguato al rischio.
La conformità del trattamento dei dati al RGDP è dimostrata attraverso l'adozione di misure di sicurezza appropriate e l'adesione a codici di condotta approvati o a un meccanismo di certificazione approvato.
Il Titolare, i Delegati, l'Amministratore del Sistema Informatico e il Responsabile della Protezione dei dati provvedono a impartire adeguate istruzioni – ciascuno nell'ambito di sua competenza – per il rispetto delle predette misure a chiunque agisca per conto loro e abbia accesso ai dati.
I nominativi e i dati di contatto del Titolare e dei Delegati, e del Responsabile della Protezione dei dati sono resi noti mediante la pubblicazione sul sito internet istituzionale del Comune, nella Sezione Amministrazione Trasparente.
I Delegati dirigenti/Responsabili del trattamento provvedono – nell'ambito delle proprie competenze – ad effettuare verifiche periodiche sulla corretta applicazione della normativa in materia di trattamento dei dati e nell'ambito delle articolazioni organizzative cui sono preposti, in accordo con i controlli specifici effettuati dal Responsabile della Protezione dei Dati.

Art. 36
Valutazione d'impatto sulla protezione dei dati- DPIA

Qualora una tipologia di trattamento – specialmente se prevede l'impiego di nuove tecnologie - comporti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, nella fase preliminare al trattamento, effettua la valutazione dell'impatto sulla protezione dei dati (di seguito solo DPIA) oggetto del trattamento.
La valutazione d'impatto ("DPIA") è il processo attraverso il quale è descritto il trattamento, e valutata la necessità e proporzionalità. Mediante questo processo si provvede alla gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
La DPIA è uno strumento importante per la responsabilizzazione in quanto sostiene il Titolare nella dimostrazione della corretta adozione delle misure corrispondenti al disposto del GDPR.
La DPIA sulla protezione dei dati personali deve essere realizzata dal Titolare prima di procedere al trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità di esso, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Per rischio si intende uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità; per gestione dei rischi si intende invece l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.
Prima di procedere alla DPIA il Titolare provvede:

a) ad effettuare o aggiornare la ricognizione dei trattamenti;

b) a valutare se il trattamento possa determinare un rischio elevato per i diritti e le libertà degli interessati.

La DPIA è richiesta in particolare nei seguenti casi:

1) se si ha una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
2) se il trattamento riguarda, su larga scala, categorie di dati personali tali da permettere di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici capaci di rivelare in modo univoco una persona fisica. E ancora, dati relativi alla salute, alla vita sessuale, all'orientamento sessuale della persona o che interessino condanne penali e a reati o misure di sicurezza;
3) se rilevati da sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Fermo restando quanto appena espresso, i trattamenti determinanti un rischio intrinsecamente elevato e per i quali può essere chiesta una DPIA sono:

1) trattamenti valutativi o di *scoring* (valutazione punteggio), compresa la profilazione e attività predittive concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
2) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati, che producono effetti giuridici sulle persone fisiche ovvero che incidono in modo analogo su dette persone fisiche;
3) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
4) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie di dati personali;
5) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto del trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
6) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
7) dati relativi a interessati vulnerabili, ossia quelle situazioni in cui la presenza di un interessato particolarmente vulnerabile comporta una tutela specifica per la quale si possa identificare la situazione di disequilibrio nel rapporto con il Titolare, come nel caso dei dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
8) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche e organizzative;
9) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Qualora il trattamento soddisfi almeno due dei criteri sopra elencati occorre, in via generale, condurre una DPIA, salvo che il Titolare, sentito il Responsabile della Protezione dei Dati e l'Amministratore del Sistema Informatico, ritenga motivatamente che non può presentare un rischio elevato. Anche in presenza di uno solo dei criteri elencati se il Titolare ha motivo di ritenerlo necessario può essere avviata una DPIA.

Il Titolare garantisce la effettuazione della DPIA ed è il responsabile della stessa. Egli ne può affidare la conduzione materiale al Responsabile della Protezione dei Dati ovvero ad un soggetto terzo interno o esterno al Comune.

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

Se l'incombenza della Valutazione è affidata all'RPD egli provvede alla sua realizzazione, qualora invece, tale

attività non sia di sua competenza diretta egli monitora sul corretto svolgimento.
I Responsabili del trattamento collaborano e assistono il Titolare e il Responsabile della protezione dei dati nella conduzione della Valutazione, redigendo per quanto di loro competenza il Registro unitario dei trattamenti e fornendo ogni informazione necessaria.
L'Amministratore del Sistema Informatico fornisce il necessario supporto al Titolare per lo svolgimento della DPIA.
Il RPD può proporre lo svolgimento della Valutazione in riferimento ad uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
L'Amministratore del Sistema Informatico può proporre di condure una DPIA in relazione ad uno specifico trattamento, con riguardo alle esigenze di sicurezza operative.

La DPIA non è richiesta nei seguenti casi:

1) 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";
2) 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;
3) se il trattamento è stato sottoposto a verifica da parte del Garante della Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;
4) qualora il trattamento sia necessario per adempiere ad un obbligo legale oppure sia necessario alla esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.
5) qualora trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro e 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.

La DPIA deve contenere almeno:

1) una descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento. Deve tenere conto dei codici di condotta approvati e indicare: i dati personali oggetto del trattamento, i destinatari, il periodo previsto di conservazione, una descrizione funzionale del trattamento, gli strumenti coinvolti nel trattamento (hardware, sotware, reti, persone, supporti cartacei o canali di trasmissione cartacei);
2) una valutazione della necessità e proporzionalità dei trattamenti in riferimento a:
    a. finalità specifiche, esplicite e legittime;
    b. liceità del trattamento;
    c. adeguatezza, pertinenza e contenimento dei dati;
    d. limite del periodo di conservazione;
    e. informazioni fornite agli interessati;
    f. diritto di accesso e portabilità dei dati;
    g. diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
    h. rapporti con i responsabili del trattamento;
    i. garanzie per i trasferimenti internazionali dei dati;
    j. consultazione preventiva con il Garante della Privacy;
3) una valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati la natura, la particolarità e la gravità/ponderazione dei

rischi.

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

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

Per conseguire l'obiettivo della riduzione del rischio la DPIA, va realizzata tenendo conto delle seguenti-fasi:

a) descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
b) valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) valutazione dei rischi per i diritti e le libertà degli interessati;
d) individuando 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 presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il Responsabile della protezione dei dati.

Art. 37
Consultazione preventiva

Laddove la DPIA riveli la presenza di rischi residui elevati, il Titolare, prima di procedere al trattamento consulta l'autorità di controllo e qualora la Valutazione indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio chiede la consultazione preventiva dell'autorità di controllo in relazione al trattamento.

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

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

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

Il Titolare, prima di procedere al Trattamento dei dati, consulta, per il tramite del RPD, il Garante qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

Qualora il Titolare ritenga che il trattamento di cui al paragrafo precedente violi il GDPR, in particolare nell'evenienza che il Titolare non abbia identificato o attenuato in maniera adeguata il rischio, l'autorità di controllo fornisce, entro otto settimane dal ricevimento della richiesta di consultazione, un parere scritto e si avvale dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'art. 58 GDPR.

Considerata la complessità del Trattamento tale periodo può essere prorogato di sei settimane. L'autorità di controllo informa il Titolare e, ove possibile, il Responsabile del Trattamento in merito alla proroga, motivando il ritardo entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere

sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.
Al momento di procedere alla consultazione come descritta al primo paragrafo del presente documento, il Titolare comunica all'autorità di controllo:

1) ove applicabili, le rispettive responsabilità del Titolare, dei contitolari e dei responsabili del trattamento;
2) le finalità e i mezzi di trattamento previsti;
3) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del GDPR;
4) i dati di contatto del Responsabile della protezione dei dati;
5) la Valutazione d'impatto sulla protezione dei dati;
6) ogni altra informazioni richiesta dall'autorità di controllo.

Art. 38
Pubblicazione sintesi della valutazione d'impatto DPIA

Il Titolare effettua la pubblicazione della DPIA o di una sua sintesi al fine di contribuire e stimolare la fiducia nei confronti dei trattamenti effettuati, nonché di dimostrare la responsabilizzazione e la trasparenza.
Le DPIA in sintesi sono pubblicate sul sito istituzionale dell'Ente, nell' apposita sottosezione "Privacy" in "Altri Contenuti" della sezione Amministrazione trasparente.

Art. 39
Modulistica e procedure

Il Titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del GDPR, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante
a) adotta e tiene costantemente aggiornati:

1. modelli uniformi di informativa;
2. modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;

b) elabora, approva, e costantemente aggiorna:

1. adeguate procedure gestionali e procedurali generali.

Art. 40
Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

Per violazione dei dati personali si intende – Data Breach – la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.
Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è sanzionato da parte del Garante della Privacy in virtù di quanto disposto dagli artt. 166 del Codice della Privacy e 83 del GDPR da parte del Garante, nonché con sanzioni di natura disciplinare.
Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi le disposizioni contenute nel presente regolamento e nella normativa di settore.
Il Responsabile del trattamento risponde per il danno causato dal trattamento solo qualora non abbia dato corso a quanto stabilito dal Codice, dal GDPR e dal presente regolamento, non adempiendo agli obblighi a lui specificamente diretti o abbia agito in modo difforme o contrario alle istruzioni legittimamente impartitegli dal Titolare del trattamento.

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

Art. 41.
Notificazione di una violazione dei dati personali

Qualora il Titolare ritenga che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede a dar notifica della avvenuta violazione al Garante della Privacy.
La notifica dovrà essere effettuata entro 72 ore e qualora la notifica non sia effettuata entro 72 ore dovrà essere corredata dei motivi del ritardo comunque senza ulteriore ingiustificato ritardo.
Il Responsabile interno del trattamento è obbligato a informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione sono:

a. danni fisici, materiali o immateriali alle persone fisiche;
b. perdita del controllo dei dati personali;
c. limitazione dei diritti, discriminazione;
d. furto o usurpazione d'identità;
e. perdite finanziarie, danno economico o sociale;
f. decifratura non autorizzata della pseudonimizzazione;
g. pregiudizio della reputazione;
h. perdita della riservatezza dei dati personali protetti dal segreto professionale (sanitari, giudiziari).

Qualora il Titolare ritenga che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, utilizzando un linguaggio semplice e chiaro al fine di far comprendere loro la natura della violazione.
I rischi per i diritti e le libertà degli interessati possono essere considerati elevati qualora la violazione:

a. coinvolga un rilevante numero di dati personali;
b. comprenda anche i dati che possono accrescere i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e alle preferenze);
c. comporti rischi imminenti o con un'elevata probabilità di accadimento (rischio di perdita finanziaria in caso di furto dei dati relativi alle carte di credito);
d. impatti su soggetti che possono essere considerati vulnerabili per le loro condizioni (utenti deboli, minori, soggetti indagati).

La notifica deve contenere almeno:

a. la descrizione della natura della violazione comprese, ove possibile, le categorie e il numero approssimativo di interessati in questione. Le categorie e il numero approssimativo delle registrazioni interessate;
b. la comunicazione del nome e dei dati di contatto del Responsabile della protezione dei dati o altro punto di contatto valido per il reperimento delle informazioni;
c. la descrizione delle probabili conseguenze della violazione;
d. la descrizione delle misure adottate o delle quali si propone l'adozione da parte del Titolare del trattamento per rimediare alla violazione e per attenuare i possibili effetti negativi;
e. le informazioni che possono essere fornite in fasi successive senza ingiustificato ritardo;

Il Titolare del trattamento ha l'onere di documentare le violazioni subite dai dati, anche se non comunicate all'Autorità di controllo, unitamente alle circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che si intende mettere in atto per porre rimedio.
Tale documentazione viene conservata con cura e diligenza e, se richiesta, messa a disposizione del Garante della Privacy al fine di attestare il rispetto delle disposizioni del RGPD.

Art. 42
Comunicazione agli interessati di una violazione dei dati personali

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
La comunicazione all'interessato del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure riportate nell'articolo precedente.
Non è richiesta la comunicazione all'interessato di cui sopra se è soddisfatta una delle seguenti condizioni:

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

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

Art. 43
Disposizioni finali

Per quanto non previsto nel presente regolamento si rinvia al predetto Regolamento europeo 2016/679, alle vigenti fonti di diritto europee e nazionali e ai regolamenti comunali in materia di protezione dei dati personali, alle linee guida e ai provvedimenti del "Gruppo di Lavoro 29" nonché del Garante della Privacy, alle direttive impartite dal Titolare del trattamento, dai Responsabili del trattamento, dall'Amministratore del sistema informatico e dal Responsabile della protezione dei dati. L'efficacia del presente regolamento decorre dal giorno in cui diviene esecutiva la deliberazione con cui è stato approvato.
Il presente regolamento, divenuto esecutivo, è pubblicato nel sito web istituzionale del Comune, nella sezione Regolamenti e nella sottosezione "Privacy" in "Altri Contenuti" della sezione Amministrazione trasparente.