# COMUNE DI BARI SARDO

## REGOLAMENTO COMUNALE
## DI ATTUAZIONE DEL REGOLAMENTO UE 2016/679
## RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE
## CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

**Approvato con Deliberazione del Consiglio Comunale n. 48 del 19.9.2018**

## TITOLO I
## PRINCIPI E DEFINIZIONI

### Art. 1 - Finalità

1. Il presente Regolamento disciplina le misure organizzative ed i processi interni di attuazione del Regolamento UE n. 679/2016 (R.G.P.D.) ai fini del trattamento di dati personali per finalità istituzionali nel Comune di Bari Sardo.
2. Ai fini del presente Regolamento, per funzioni istituzionali si intendono quelle:
a) previste dalla legge, dallo statuto comunale e dai regolamenti;
b) esercitate in attuazione di convenzioni, accordi nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente;
c) svolte per l'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'Ente locale;
d) in esecuzione di un contratto con i soggetti interessati;
e) per finalità specifiche e diverse dai punti precedenti purché l'interessato esprima il consenso al trattamento.
3. Il presente Regolamento è conforme alle norme e principi costituzionali nonché alle altre disposizioni vigenti sulla materia, incluse le norme del Codice della Privacy, D.Lgs. n.196/2003, non incompatibili rispetto al Regolamento UE n. 679/2016 (R.G.P.D.).

### Art. 2 - Principi del trattamento

1. Per le finalità indicate all'art. 1, il Comune tratta i dati personali nel rispetto dei principi di cui all'art. 5 del Regolamento UE 679/2016 e deve essere in grado di comprovarlo ("responsabilizzazione").
2. In attuazione del comma 1, i dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE 679/2016, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente Regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza).
3. Relativamente al trattamento di dati personali di persone decedute, il diritto alla riservatezza si estingue con la morte del titolare.

## Art. 3 - Definizioni

1. Ai fini del presente Regolamento si intende per:
a) "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;
b) "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;
c) "dati particolari": dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché la trattazione di 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.
d) "dati giudiziari": dati personali relativi alle condanne penali e ai reati e alle connesse misure di sicurezza;
e) "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;
f) "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;
g) "autorizzati di I livello /o designati": responsabili di settore / O.P. autorizzati a compiere operazioni di trattamento di dati personali dal titolare;
h) "autorizzati di II livello /o incaricati": il dipendente della struttura organizzativa del Comune, incaricato dal responsabile del servizio (autorizzato al trattamento di I livello), per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento (elabora o utilizza materialmente i dati personali);
i) "interessato": la persona fisica, cui si riferiscono i dati personali;
l) "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;
m) "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;
n) "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;
o) "dato anonimo": il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
p) "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;

q) “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;
r) "Garante": l'autorità preposta al controllo della privacy;
s) “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;
t) “pseudonimizzazione”: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

## TITOLO II

## SOGGETTI DEL TRATTAMENTO

### Art. 4 – Titolare del trattamento

1. Il Titolare del trattamento dei dati personali è il Comune di Bari Sardo, nella persona dal Sindaco *pro tempore* o persona delegata.
2. Il Titolare è responsabile del rispetto dei principi contenuti nell’art. 5 del Regolamento UE 679/2016: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza, inoltre deve essere in grado di comprovare gli stessi(“responsabilizzazione”).
3. Il Titolare adotta misure appropriate per fornire all’interessato le informazioni sul trattamento dei propri dati personali di cui agli artt. 13 e 14 del Regolamento UE 2016/679.
4. Il Titolare provvede altresì a:
a) designare gli autorizzati (di I livello)/designati al trattamento, nelle persone dei Responsabili di servizio in cui si articola l’organizzazione comunale che sono preposti al trattamento dei dati contenuti nelle banche dati (informatizzate e/o cartacee) esistenti nelle articolazioni organizzative di loro competenza;
b) nominare il Responsabile della protezione dei dati (DPO);
c) nominare, quali Responsabili (esterni) del trattamento, i soggetti pubblici o privati affidatari di attività e servizi per conto dell’Amministrazione comunale, che dovranno trattare dati personali per conto del Titolare nell’ambito del servizio esternalizzato (art. 28 comma 3 Regolamento UE 2016/679);
d) nominare (ove non effettuato) un Amministratore di sistema a cui spetta il compito di supportare il Titolare nel mettere in atto le misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento UE 27 aprile 2016 n.679);
e) tenere il registro delle attività di trattamento ai sensi dell’art. 30, comma 1 del Regolamento UE 2016/679;
f) istituire il registro delle violazioni e documentare al suo interno qualsiasi violazione di dati personali (ivi comprese quelle non notificate al Garante né comunicate agli interessati), comprese le circostanze ad esso relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio;
g) notificare all’Autorità di Controllo le violazioni di dati personali che presentino un rischio per i diritti e le libertà delle persone fisiche, senza ingiustificato ritardo e, in ogni caso, entro 72 ore dalla conoscenza, nonché comunicarle all’interessato ove suscettibili di presentare un rischio elevato per i diritti e le libertà;

h) effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali ("DPIA") ex art. 35 Regolamento 2016/679 nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

**Art. 5 - Autorizzati al trattamento di I livello/designati**

1. Il Titolare del trattamento dei dati nomina, con apposito decreto, più autorizzati (di I livello)/designati al trattamento, ciascuno in riferimento ad uno dei Servizi dell'Ente.
2. I soggetti autorizzati, scelti tra i titolari di Posizioni Organizzative in possesso di adeguata conoscenza specialistica, esperienza, capacità ed affidabilità per il trattamento dei dati provvedono, nell'ambito dei trattamenti affidatigli, a tutte le attività previste dalla legge e a tutti i compiti assegnati dal Titolare, analiticamente specificati per iscritto nell'atto di designazione ed in particolare a:
a) nominare gli autorizzati di II livello/incaricati al trattamento dei dati nell'ambito della propria unità operativa;
b) garantire che tutti gli autorizzati di II livello/incaricati al trattamento assicurino la riservatezza nonché siano in possesso di apposita formazione;
c) coinvolgere, insieme al Titolare del trattamento, il Responsabile della protezione dati nelle questioni relative al trattamento di dati personali;
d) riferire al Titolare del trattamento ogni violazione di dati personali (*data breach*) di cui viene a conoscenza senza ritardo ed assisterlo nel procedimento di notifica al Garante;
e) fornire assistenza al Titolare del trattamento per le comunicazioni all'interessato relative alle violazioni dei dati personali;
f) gestire, per conto del Titolare del trattamento, il registro delle attività svolte dal proprio Servizio/Settore;
g) collaborare con il Titolare alle richieste di accesso, di limitazione ed opposizione degli interessati relative a trattamenti di dati personali;
h) attuare, insieme al Titolare del trattamento, misure organizzative e tecniche adeguate per garantire un adeguato livello di sicurezza, nonché collaborare alla procedura di valutazione di impatto sulla protezione dei dati (D.P.I.A.).

**Art. 6 - Autorizzati al trattamento di II livello/incaricati**

1. Ogni Autorizzato di primo livello/designato può nominare autorizzati al trattamento di II livello (incaricati) per settori specifici con determina che:
a) individua e delimita specificatamente l'ambito del trattamento consentito;
b) contiene specifiche istruzioni in materia di sicurezza del trattamento;
c) individua le competenze dell'autorizzato/incaricato tra le quali in particolare: la comunicazione agli interessati dell'informativa relativa al trattamento dei dati e alla loro diffusione; la collaborazione alle richieste di accesso, di limitazione ed opposizione degli interessati relative a trattamenti di dati personali effettuati dal Servizio di propria competenza.
2. La nomina degli autorizzati di II livello/incaricati va comunicata al Sindaco che deve essere informato di ogni successiva variazione o sostituzione.
3. Gli autorizzati di II livello/incaricati operano sotto la diretta responsabilità del proprio Responsabile di servizio/autorizzato di I livello che li ha nominati**.** In caso di loro inadempimento risponde verso il Comune l'autorizzato di I livello.

**Art. 7 - Responsabili esterni di trattamento**

1. Il Titolare può avvalersi, per il trattamento di dati, di soggetti pubblici o privati quali responsabili esterni del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative

adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento Europeo e garantisca la tutela dei diritti e delle libertà dell'interessato. La nomina avviene mediante contratto o altro atto giuridico in forma scritta che vincoli il responsabile esterno del trattamento al Titolare e che disciplini la materia oggetto di nomina, la durata del trattamento, la natura e la finalità perseguita, la tipologia dei dati e le categorie degli interessati, gli obblighi e i diritti del Titolare del trattamento.
2. I contratti di nomina di cui al comma 1 prescrivono in capo al Responsabile del trattamento gli obblighi di cui all'art. 28 comma 3 del Regolamento 2016/679; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione Europea.

**Art. 8 - Responsabile della protezione dei dati (DPO)**

1. Il Titolare, con suo provvedimento, nomina il Responsabile della protezione dei dati (DPO), in funzione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di controllo a lui affidati.
2. Il Responsabile della protezione dei dati può essere un dirigente/funzionario in posizione apicale oppure un incaricato esterno che potrà assolvere i suoi compiti in base a un contratto di servizio.
3. Il nominativo ed i dati di contatto del Responsabile della protezione dei dati sono comunicati al Garante della protezione dei dati personali. I soli dati di contatto (mail / pec e numero di telefono) sono pubblicati sul sito istituzionale del Comune nella sezione Amministrazione trasparente.
4. Il Responsabile della protezione dei dati deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e gli vanno fornite le risorse necessarie per assolvere tali compiti, accedere ai dati personali, ai trattamenti e per mantenere la propria conoscenza specialistica.
5. Non può essere rimosso o penalizzato a causa dell'adempimento dei propri compiti.
6. I cittadini possono contattare il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente Regolamento.
7. Il Responsabile della protezione dei dati è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri deve svolgere almeno le seguenti funzioni:
a) informare e fornire consulenza al Titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
f) considerare nell'esecuzione dei propri compiti i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
g) fornire un parere al Titolare del trattamento in caso di *data breach*.
8. I compiti attribuiti al DPO sono indicati in apposito contratto di servizi. L'incarico di DPO può essere affidato anche ad un unico soggetto designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal D.Lgs. 18 agosto n. 267 del 18.8.2000 e ss. mm..

## TITOLO III

## TRATTAMENTO DEI DATI PERSONALI

### Art. 9 – Registro delle attività di trattamento

1. Il Titolare del trattamento istituisce e tiene aggiornato, in forma scritta, un registro delle attività di trattamento svolte sotto la propria responsabilità, tramite i Responsabili di Servizio, autorizzati al trattamento di I livello.
2. Il Registro delle attività di trattamento, ai sensi dell'art. 30, comma 1, del Regolamento UE 2016/679, deve contenere almeno le seguenti informazioni:
– estremi identificativi e di contatto del Titolare del Trattamento;
– estremi identificativi e di contatto del Responsabile della protezione dei dati;
– finalità del trattamento;
– descrizione delle categorie di interessati;
– descrizione delle categorie di dati personali;
– categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
– eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale con documentazione delle garanzie in materia di privacy;
– termini ultimi previsti per la cancellazione delle diverse categorie di dati;
– descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
3. In caso di richiesta del Garante, il Registro di cui al secondo comma, è messo immediatamente a disposizione.

### Art. 10 – Trattamento di dati particolari

1. Gli Uffici del Comune di Bari Sardo trattano i dati particolari, ai sensi dell'art. 9 del Regolamento UE 2016/679, che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici, relativi alla salute, alla vita sessuale nei seguenti casi:
a) ove l'interessato abbia 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, ex art.9 del Regolamento UE 2016/679;
b) ove il trattamento sia 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) ove il trattamento sia 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) ove il trattamento sia 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) ove il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato;
f) ove il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) ove il trattamento sia 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) ove il trattamento sia 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, ex art.9 del Regolamento UE 2016/679;
i) ove il trattamento sia 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) ove il trattamento sia 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 Regolamento UE 2016/679, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
2. I dati particolari sono trattati sempre nel rispetto dei principi di cui all'art. 5 del Regolamento UE 2016/679, ovvero devono essere esatti, pertinenti, non eccedenti ed indispensabili rispetto alle finalità perseguite e aggiornati. In tutti i casi indicati vanno sempre previste misure di garanzia appropriate e specifiche per tutelare i diritti fondamentali e gli interessati. A tal fine si applicano le misure di sicurezza previste nei successivi artt. 14 e ss del presente Regolamento.
3. I dati particolari riguardanti lo stato di salute non devono essere divulgati.
4. Gli uffici del Comune di Bari Sardo trattano dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1 del Regolamento UE 2016/679, soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

**Art. 11 - Pubblicazione web Amministrazione Trasparente e Albo pretorio**

1. Il Comune di Bari Sardo effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti dal D.Lgs. n. 33/2013 e ss. mm., nonché sull'Albo pretorio online ai sensi dell'art. 32 della L. 69/2009.
2. I documenti di cui al D.lgs n. 33/2013 e ss. mm. sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e vanno mantenuti aggiornati.
3. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.
4. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza, mentre possono essere diffusi per le altre finalità solo se indispensabili.
5. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.
6. I dati vanno pubblicati in formato di tipo aperto ai sensi dell'art. 1, comma 1, D. Lgs. 217/2017 e sono liberamente riutilizzabili secondo la normativa vigente. I dati personali diversi dai dati particolari e dai dati

giudiziari, possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web.
7. I dati, le informazioni e i documenti di cui al comma 1, sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione.
8. Deroghe alla predetta durata temporale quinquennale sono previste:
a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;
b) per alcuni dati e informazioni riguardanti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale ai sensi dell'art. 14, comma 2, D.Lgs. n. 33/2013 e ss. mm. e i titolari di incarichi dirigenziali e di collaborazione o consulenza che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell'incarico ai sensi dell'art. 15, comma 4, D.Lgs. n. 33/2013 e ss. mm.;
c) nel caso in cui siano previsti diversi termini dalla normativa in materia di trattamento dei dati personali.
9. I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali nel rispetto di quanto statuito dall'art. 24 del presente Regolamento.
10. Il Comune prima di procedere con la pubblicazione sull'albo pretorio online dei degli atti amministrativi contenenti dati personali, ivi compresi i dati particolari o giudiziari, deve verificare l'esistenza di una norma di legge che imponga tale affissione.
11. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione e non possono essere mai pubblicati dati idonei a rivelare lo stato di salute;
12. Una volta trascorso il periodo temporale previsto dalle singole discipline per la pubblicazione degli atti e documenti nell´albo pretorio, il Comune non può continuare a diffondere i dati personali in essi contenuti.
Ove il Comune di Bari Sardo volesse continuare a mantenere nel proprio sito web istituzionale gli atti e i documenti pubblicati, ad esempio nelle sezioni dedicate agli archivi degli atti e/o della normativa dell´ente, dovrà apportare gli opportuni accorgimenti per la tutela dei dati personali. In tali casi, quindi, è necessario provvedere a oscurare nella documentazione pubblicata i dati e le informazioni idonei a identificare, anche in maniera indiretta, i soggetti interessati.
13. Il Comune di Bari Sardo nell'assolvere ai propri obblighi di pubblicazione degli atti nell´albo pretorio online, deve adottare gli opportuni accorgimenti tecnici per evitare l´indicizzazione nei motori di ricerca generalisti della documentazione contenente dati personali pubblicata.
14. Per quanto non espressamente indicato nel presente Regolamento si fa espresso rinvio alle disposizioni normative di riferimento, nonché alle linee guida del Garante in materia di trattamento dei dati personali contenuti in atti e documenti amministrativi effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici (allegato alla deliberazione n. 243 del 15 maggio 2014).

### Art. 12 - Pertinenza delle informazioni contenenti dati personali

1. Non possono essere disposti filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente". Al contrario l'Albo pretorio non deve essere indicizzato.
2. Qualora i dati personali contenuti nei documenti non siano pertinenti o siano eccedenti rispetto all'interesse manifestato dal richiedente nell'istanza di ostensione, al fine di salvaguardare la riservatezza di terzi, l'accesso agli atti può essere limitato, su valutazione del Responsabile del procedimento, mediante l'occultamento di alcuni contenuti.

### Art. 13 - Trattamento dei dati personali effettuato con sistemi di videosorveglianza

1. Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza richiede apposita informativa agli interessati e questa può essere rilasciata in forma semplificata purché faccia espresso richiamo ad una informativa completa recante le indicazioni di cui agli artt. 13 e 14 del Regolamento UE 679/2016, pubblicata in apposita sezione del sito internet istituzionale.
2. Per finalità di tutela della sicurezza urbana, la durata della conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione" in conformità dell'art. 6, co. 8, D.L. n. 11/2009. Negli altri casi, la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione.
3. Ai dati raccolti mediante sistemi di videosorveglianza, vanno applicate misure di sicurezza adeguate ai sensi dell'art. 20 del presente Regolamento.
4. Il Comune di Bari Sardo deve assicurare agli interessati identificabili l´effettivo esercizio dei propri diritti in conformità al GDPR, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.
5. Per il trattamento di dati personali effettuato mediante sistemi di videosorveglianza, per quanto non previsto nel presente Regolamento, si fa espresso rinvio al provvedimento del Garante 8 Aprile 2010 in quanto compatibile, nonché al Regolamento in materia di videosorveglianza eventualmente redatto dal Comune di Bari Sardo.

## TITOLO IV

## MISURE DI SICUREZZA

### Art. 14 - Misure di sicurezza preventive

1. Il Comune di Bari Sardo deve adottare misure che soddisfino la protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita; ovvero, mette in atto misure tecniche ed organizzative adeguate sia prima del trattamento, sia nell'atto del trattamento stesso indicate nel presente titolo.
2. Il Comune di Bari Sardo, in particolare:
– utilizza le tecniche di pseudonimizzazione dei dati personali;
– tratta i soli dati necessari per ogni specifica finalità al fine di garantire la massima protezione dei dati attraverso il loro minimo trattamento;
– custodisce e controlla i dati personali in modo da ridurre al minimo, mediante l'adozione di misure di sicurezza preventive, i rischi di distruzione, perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità pubbliche di raccolta;
– provvede a formare il personale sugli obblighi in materia di protezione dei dati personali in relazione alle specifiche competenze rivestite dai singoli dipendenti e dai rispettivi uffici in cui sono inseriti.
3. Il Comune di Bari Sardo favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e degli autorizzati al trattamento.

### Art. 15 – Valutazione d'impatto (D.P.I.A.)

1. Oltre le misure preventive di cui all'articolo precedente, il Comune di Bari Sardo quando un trattamento presenta a seguito di analisi, rischi elevati per i diritti e le libertà degli interessati, procede, prima del trattamento, alla valutazione di impatto sulla protezione dei dati (D.P.I.A.).
2. La D.P.I.A. può riguardare una singola operazione di trattamento o due o più trattamenti simili che presentano rischi elevati analoghi.

3. Ricorrono rischi elevati ai sensi dell'art. 35, par. 3, Reg. UE 679/2016 in presenza di:
– una valutazione sistematica di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su tali persone fisiche;
– trattamento su larga scala, di categorie particolari di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, relativi alla salute, alla vita sessuale o condanne penali, a reati e misure di sicurezza;
– sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4. In caso ricorra uno dei tre indici di cui al comma precedente il Comune di Bari Sardo deve procedere ad effettuare la D.P.I.A.
5. Il Comune altresì redige una valutazione di impatto del rischio se ricorrono due dei seguenti indici forniti dal Garante:
– decisioni automatizzate che producono significativi effetti giuridici o di altra natura;
– monitoraggio sistematico;
– valutazione o assegnazione di un punteggio inclusiva di profilazione, in particolare in considerazione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
– dati sensibili o di carattere estremamente personale;
– trattamento di dati su larga scala;
– creazione di corrispondenze o combinazione di insiemi di dati;
– dati relativi a interessati vulnerabili considerato lo squilibrio di potere tra gli interessati ed il Comune;
– uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto;
– trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contrattato;
6. Il Titolare, se lo ritiene opportuno, può procedere anche alla D.P.I.A. in caso ricorra anche uno solo dei requisiti sopra indicati e può individuare anche altri criteri di riscontro del rischio elevato in base alla specifica circostanza.

## Art. 16 - Procedimento

1. Qualora ricorra un rischio elevato il Comune, Titolare del trattamento, chiede il parere del Responsabile della Protezione dei dati e, se lo ritiene opportuno, dei portatori di interessi.
2. La D.P.I.A. deve presentare il seguente contenuto minimo:
– una descrizione dei trattamenti previsti e delle finalità del trattamento;
– una valutazione della necessità e proporzionalità dei trattamenti;
– una valutazione dei rischi per i diritti e le libertà degli interessati;
– le misure previste per affrontare i rischi.
3. La D.P.I.A. può essere effettuata anche per il tramite degli autorizzati al trattamento di I livello ma la responsabilità finale è del Titolare del trattamento.
4. In caso la D.P.I.A. non riesca a trattare in maniera sufficiente i rischi individuati, per quelli residui va effettuata la consultazione del Garante da parte del Titolare del trattamento ex art. 36 GDPR.
5. Il Comune, Titolare del trattamento, provvede a pubblicare sul proprio sito istituzionale, nella sezione Amministrazione Trasparente, una sintesi della DPIA ovvero una dichiarazione nella quale si afferma che la DPIA è stata condotta, al fine di rafforzare la fiducia da parte degli interessati in merito ai trattamenti effettuati ed altresì per dimostrare il pieno rispetto di principi quali la responsabilizzazione e la trasparenza.

## Art. 17 - Consultazione preventiva del Garante della privacy

1. Nei casi in cui si è proceduto nella valutazione di impatto sulla protezione dei dati ed è emerso che il Comune non riesce a trattare in maniera sufficiente tutti i rischi elevati, poiché ne restano ancora alcuni per questi ultimi residui, va consultato preventivamente il Garante per la privacy.
2. Il Comune di Bari Sardo invia richiesta di consultazione al Garante comunicando:
– i dati dell'Ente Locale in quanto Titolare del trattamento e i dati di contatto del Responsabile della protezione dati;
– le finalità ed i mezzi di trattamento previsti;
– le misure di garanzia previste per proteggere i diritti e le libertà fondamentali degli interessati;
– la valutazione di impatto sulla protezione dei dati in versione completa;
– ogni altra informazione ritenuta necessaria.
3. Il Garante formula parere scritto entro otto settimane dal ricevimento della richiesta di consultazione nel caso in cui ritenga che il trattamento comunicato violi le norme sulla protezione dei dati ed in particolare qualora ritenga che il Comune non abbia sufficientemente attenuato o identificato il rischio. In base alla complessità del trattamento previsto il Garante può prorogare la sua risposta di un termine aggiuntivo di sei settimane informando il Responsabile della protezione dei dati, entro un mese dal ricevimento della richiesta di consultazione.
4. In caso sia necessario il Garante può richiedere al Responsabile della protezione dei dati informazioni aggiuntive a quelle già comunicate e può sospendere la decorrenza dei termini di cui al comma 3 in attesa della loro trasmissione.
5. In assenza di parere espresso del Garante entro le otto settimane dal ricevimento della richiesta di consultazione, il Comune può procedere nel trattamento dei dati.

**Art. 18 - Misure di sicurezza per trattamenti con strumenti elettronici ed informatici**

1.Il Comune di Bari Sardo, nella sua qualità di Titolare del trattamento dei dati personali, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, il Comune deve tener conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato o a un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al comma 1 del presente articolo.
4. Il titolare del trattamento e i responsabili esterni del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

**Art. 19 - Misure per trattamenti non automatizzati**

1. Il Comune di Bari Sardo fornisce istruzioni scritte agli autorizzati di I livello ed agli autorizzati di II livello/incaricati anche per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici, in particolare, per il controllo e la custodia, per intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
2. I documenti che contengano dati particolari e giudiziari, sono controllati fino alla restituzione in modo che non accedano ad essi persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
3. L'accesso agli archivi contenenti dati particolari o giudiziari è controllato.
4. Le persone ammesse, dopo l'orario di chiusura, sono identificate e registrate e se mancano strumenti elettronici di controllo degli accessi agli archivi, questi vanno preventivamente autorizzati.

**Art. 20 - Misure per dati raccolti con sistemi di videosorveglianza**

1. I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con adeguate misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini, nel pieno rispetto della protezione dei dati sin dalla progettazione e per impostazione predefinita. Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l´attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica autorizzato al trattamento)
2. Occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando – quando non indispensabili – immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
3. Devono quindi essere adottate almeno le seguenti specifiche misure tecniche ed organizzative:
– in presenza di differenti competenze attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati autorizzati al trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
– laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
– per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto, anche mediante sovraregistrazione, con modalità tali da non rendere riutilizzabili i dati cancellati;
– nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
– qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo.

– la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs).
4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza predisponendo apposita informativa semplificata (cartellonistica) che richiami ad una informativa dettagliata redatta *ex* artt. 13 e 14 del Regolamento UE 679/2016 , nonché va determinato con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione.

**Art. 21 - Sistema e politica di audit**

1. Il Comune di Bari Sardo mette in atto misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è conforme al Regolamento UE 679/2016 e, a tal fine, adotta il procedimento di audit in conformità anche delle politiche della qualità.
2. Il Comune di Bari Sardo tramite il Responsabile della protezione dei dati, valuta, mediante audit, i processi interni all'ente locale per:
– verificare il grado di conformità del trattamento dei dati personali effettuato da tutti gli uffici alla normativa vigente;
– verificare che tutti i dipendenti osservino le regole per la liceità e la sicurezza del trattamento di dati personali;
– verificare l'efficacia di azioni correttive a seguito di "non conformità".
3. Il processo consiste:
– in una prima mappatura delle possibili situazioni di rischio che si verificano nel Comune in base alla sua organizzazione interna, agli uffici ed al trattamento dei dati di ciascuno;
– nell'individuare situazioni di non conformità del trattamento agli standard di sicurezza come anche previsti nel presente titolo;
– nel porre in essere azioni correttive.
4. Il processo del comma precedente, dopo la prima volta che è stato effettuato, si sviluppa in monitoraggi periodici di verifica dell'applicazione delle misure stabilite e nella sostituzione o riesame delle misure per il miglioramento dei trattamenti da parte dei vari uffici del Comune. In particolare nel corso degli audit viene verificato che:
– venga fatto un uso corretto di mezzi informatici ai fini del trattamento dei dati personali, in particolare monitorando l'utilizzo delle password e gli accessi agli archivi elettronici contenenti dati personali con particolare attenzione ai dati particolari;
– venga fatto un corretto utilizzo degli archivi cartacei che conservano i dati personali con particolare riguardo alla conservazione dei dati particolari;
– vengano adeguatamente formati i dipendenti in modo diversificato in base alla modalità di trattamento cui sono preposti;
– ogni ufficio comunale tratti i dati secondo il principio di minimizzazione, ovvero, solo a ciò che sia strettamente necessario, si accerti dell'esattezza e correttezza dei dati e che conservi i dati nel rispetto dei termini indicati dalle norme, laddove presenti, o, in subordine per il tempo strettamente necessario al raggiungimento della finalità di trattamento;
– in caso di incidenti o violazioni come descritte al titolo successivo, siano applicate le misure correttive per porre riparo agli effetti negativi;
– siano garantiti i diritti degli interessati e correttamente curate le istanze di accesso, cancellazione, limitazione del trattamento, rettifica nonché siano verificate le istanze di opposizione nonché i reclami eventualmente presentati al Garante;

– vengano tenuti sempre aggiornati i contenuti delle informative e siano adattate alle esigenze dei differenti uffici e differenti trattamenti;
– i documenti contenenti dati personali, presenti nel sito internet del Comune con particolare riferimento alla pubblicazione all'albo pretorio ed alla sezione Amministrazione Trasparente siano conformi ai tempi di pubblicazione previsti dall'art. 124, del D.Lgs. n. 267/2000 e ss. mm. e del D.Lgs. n. 33/2013 e ss. mm.;
– nelle ipotesi di utilizzo di sistemi di videosorveglianza vengano rispettate le specifiche misure di sicurezza come indicate all'art. 20 del presente Regolamento.

## TITOLO V

## DIRITTI DELL'INTERESSATO

### Art. 22 - Diritto di accesso

1. L'interessato ha sempre diritto di ottenere dal Titolare del trattamento la conferma che sia in corso un trattamento dei dati personali che lo riguardano e, in tal caso, di averne accesso e di acquisire le seguenti informazioni:
a) finalità del trattamento;
b) categoria di dati trattati;
c) i destinatari o la categoria di destinatari a cui i dati personali sono o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) il periodo di conservazione dei dati previsto o se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del proprio diritto a richiedere la rettifica o cancellazione del dato o la limitazione del trattamento dei dati o di opporsi al loro trattamento;
f) il diritto a proporre reclamo all'autorità di controllo;
g) tutte le informazioni possibili sull'origine dei dati non raccolti presso l'interessato;
h) l'esistenza di un processo automatizzato compresa la profilazione e, in tali casi, informazioni sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. La richiesta va inoltrata in forma scritta dall'interessato ricorrendo all'apposita modulistica pubblicata nel sito istituzionale del Comune; in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.
3. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
4. I soggetti autorizzati al trattamento e gli incaricati, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole. In tale ipotesi, va rilasciata copia del documento richiesto.
5. Il rilascio della copia è gratuito; in caso di richiesta di copie ulteriori il rilascio può essere subordinato al pagamento di un contributo per costi amministrativi, anche nel caso in cui le richieste risultino infondate o eccessive, in particolare per il loro carattere ripetitivo.

### Art. 23 - Diritto alla rettifica dei dati

1. L'interessato ha diritto a chiedere previa richiesta scritta, la rettifica da parte del Comune, senza ingiustificato ritardo, dei dati personali inesatti che lo riguardano. La rettifica include anche la possibile integrazione dei dati avuto riguardo alla finalità del trattamento.

2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
3. I soggetti autorizzati al trattamento e gli incaricati, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, anche al fine di identificarlo e, successivamente, per dare seguito all'esercizio del diritto dell'interessato.

**Art. 24 - Diritto all'oblio**

1. L'interessato ha diritto a chiedere previa richiesta scritta, al Titolare del trattamento la cancellazione dei dati personali che lo riguardano ove siano illecitamente trattati.
2. Tale diritto non si applica nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) 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;
c) 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;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

**Art. 25 - Diritto di limitazione**

1. L'interessato, previa richiesta scritta, ha diritto ad ottenere dal Titolare del trattamento la limitazione del trattamento:
– in caso sia contestata l'esattezza dei dati personali, per il periodo necessario alla verifica da parte del Comune;
– in caso di trattamento illecito, se si oppone alla cancellazione dei dati chiedendo invece che ne sia limitato l'utilizzo;
– in caso di esercizio di opposizione nell'attesa della verifica dei presupposti del relativo diritto.
2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
3. Gli autorizzati al trattamento e gli incaricati, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.
4. In caso di riscontro favorevole va comunicato all'interessato che ha ottenuto la limitazione del trattamento, senza ritardo e prima che la limitazione sia revocata nei casi di cui ai commi 1 e 3. Vanno altresì avvisati i destinatari della limitazione dei dati, salvo ciò non sia impossibile o richieda uno sforzo sproporzionato.

**Art. 26 – Diritto alla portabilità**

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

## Art. 27 - Diritto di opposizione

1. L'interessato può presentare per iscritto richiesta di opposizione al trattamento dei dati personali che lo riguardano per motivi connessi alla sua situazione particolare, inclusa la profilazione.
2. Il Titolare del trattamento entro trenta giorni fornisce risposta all'interessato a seguito della valutazione della situazione: è consentito l'esercizio del diritto se non esistano comprovati motivi basati su norma di legge per procedere al trattamento prevalenti sugli interessi del richiedente o se si tratta di esercizio o accertamento di un diritto in sede giudiziaria.
3. Il termine di cui al precedente comma può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.
4. I soggetti autorizzati al trattamento e gli incaricati, sono tenuti a collaborare nel procedimento interno di verifica dei presupposti del diritto di opposizione.
5. In ogni comunicazione all'interessato deve essere inserito l'avviso in modo chiaro e separato dal restante contenuto dell'atto che questi può esercitare il diritto all'opposizione.

## Art. 28 - Obbligo di informativa

1. Nel momento in cui i dati personali sono ottenuti, ovvero, nell'ipotesi di dati personali raccolti presso terzi, entro i termini indicati dall'art.14, par.3 Reg. UE 679/2016, il Titolare del trattamento fornisce all'interessato le informazioni di cui agli artt. 13 e 14 del Reg. UE 679/2016 necessarie per consentirgli l'esercizio dei propri diritti.
2. L'informativa privacy deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.
3. Non è necessario fornire l'informativa:
– nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;
– nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.
In tali casi il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni.
4. In presenza di un obbligo di legge che impone la riservatezza e segretezza dei dati personali.

## 29 - Contenuto dell'informativa

1. L'informativa è gratuita e deve essere sintetica, presentare un linguaggio chiaro e semplice ed essere in ogni caso comprensibile per l'interessato.
2. Essa presenta il seguente contenuto:
– indicazione dell'identità e dei dati di contatto del Titolare del trattamento;
– indicazione dei dati di contatto del Responsabile della protezione dei dati;
– indicazione di ogni finalità istituzionale di trattamento e della base giuridica del trattamento;
– indicazione delle categorie dei dati personali trattati;
– indicazione delle modalità di trattamento distinte anche in base all'ufficio del Comune che lo effettua evidenziando se sia un trattamento automatizzato (con eventuale possibilità di profilazione e della sua logica) o se sia un trattamento cartaceo;
– indicazione degli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
– ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, Reg.

UE 679/2016, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
– il periodo di conservazione dei dati personali e, se non è previsto da norma di legge, il criterio utilizzato dal Titolare per la durata del trattamento;
– l'indicazione dei diritti che l'interessato può esercitare, ovvero: accesso, integrazione e rettifica, eventuale revoca, opposizione nonché la possibilità di presentare reclamo all'Autorità di controllo;
– le conseguenze in caso di rifiuto del trattamento o di omessa comunicazione di dati;
– l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Il Titolare del trattamento può di volta in volta aggiungere ogni ulteriore informazione che si ritiene necessaria al caso concreto.

**Art. 30 - Informativa per utilizzo di sistemi di videosorveglianza**

1. Nel caso di utilizzo di sistemi di videosorveglianza, gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).
2. A tal fine può essere utilizzato un modello di informativa "minima" semplificata che poi rinvii a un testo contenente tutti gli elementi completi di cui agli artt. 13 e 14 del Regolamento UE 679/2016, disponibile agevolmente senza oneri per gli interessati, sia nel sito internet dell'amministrazione comunale sia affisso negli uffici comunali.
3. In ogni caso il Titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'articolo precedente.
4. Il supporto con l'informativa minima:
– deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
– deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
– può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

**Art. 31 - Consenso**

1. Il consenso al trattamento dei dati non è richiesto al Comune di Bari Sardo in quanto Pubblica Amministrazione se agisce per finalità istituzionali.
2. Il consenso può essere richiesto se il Comune agisce per specifiche finalità diverse da quelle istituzionali ai sensi dell'art. 1, comma 1, lett. e). In tal caso il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.
3. La richiesta di consenso deve essere comprensibile, facilmente accessibile, chiara e semplice.
4. Il consenso può essere revocato ed in tal caso la revoca non pregiudica la liceità del trattamento già effettuato. Il consenso è revocato con la stessa facilità con cui è stato prestato.
5. Se il consenso dell'interessato al trattamento 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 Regolamento UE 679/2016 e del presente Regolamento è vincolante.

## TITOLO VI

## DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

### Art. 32 - Violazione dati personali (data breach)

1. La violazione dei dati personali comporta una compromissione della sicurezza che determina, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali.
2. Gli autorizzati al trattamento di II livello/incaricati al trattamento che vengano a conoscenza di una violazione di dati personali ne danno immediata notizia al responsabile di unità operativa/autorizzato al trattamento di I livello il quale dovrà provvedere a darne tempestiva comunicazione al Titolare.
3. In caso di violazione dei dati personali, il titolare del trattamento richiede immediato parere al Responsabile della protezione dei dati sulla gravità della violazione.
4. Al Titolare del trattamento compete la valutazione finale sulla gravità o meno della violazione. In caso venga riscontrata la presenza di rischi per le persone fisiche va effettuata via Pec la notifica del *data breach* al Garante per la privacy entro 72 ore dal momento in cui ne è venuto a conoscenza o, se in un momento successivo, nel provvedimento vanno indicati i motivi del ritardo.
5. Nel caso in cui la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare procede a darne comunicazione all'interessato.
6. Il Titolare del trattamento potrebbe omettere la notifica di cui al comma 3 qualora sia improbabile che la violazione possa comportare un rischio per i diritti e le libertà degli interessati. Ciò si verifica qualora il Comune, al momento in cui essa si è verificata, aveva misure di sicurezza che hanno reso i dati inintellegibili perché per esempio anonimi o cifrati in modo sicuro attraverso un algoritmo standardizzato o mediante schemi di cifratura a chiave simmetrica. Non ricorre l'inintellegibilità se la violazione ha portato la distruzione o perdita dei dati personali.

### Art. 33 - Notifica al Garante della privacy

1. La notifica al Garante deve presentare il seguente contenuto minimo:
– descrivere la natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
– indicare il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
– descrivere le probabili conseguenze della violazione dei dati personali;
– descrivere le misure adottate o di cui si propone l'adozione da parte del Comune per porre rimedio alla violazione dei dati personali.
A questo contenuto minimo è possibile aggiungere ogni altra informazione che il Titolare ritiene necessaria.
2. In caso non si sia in possesso delle informazioni di cui al comma 1 il Titolare procederà a comunicare entro 72 ore quelle di cui è a conoscenza e successivamente, appena verrà in possesso dei dati mancanti, effettuerà una comunicazione integrativa senza ingiustificato ritardo.
3. Il Garante può indicare l'adozione di misure integrative a quelle già descritte nella notifica, oltre che fornire osservazioni per porre rimedio alla violazione e può anche imporre la comunicazione all'interessato di cui al successivo articolo, qualora non sia stata ritenuta necessaria dal Comune.

### Art. 34 - Comunicazione all'interessato

1. Il Titolare del trattamento comunica, senza ingiustificato ritardo, all'interessato la violazione in presenza solo di rischio elevato per i diritti e le libertà delle persone fisiche.

2. La comunicazione all'interessato va effettuata con un linguaggio semplice e chiaro e deve presentare anch'essa un contenuto minimo rappresentato da:
– il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
– le probabili conseguenze della violazione dei dati personali;
– le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali.
3. In caso non ricorrano i presupposti per la notifica al Garante come indicati dall'articolo precedente, non si procede nemmeno alla comunicazione all'interessato.
Questa inoltre non è necessaria se:
– i dati violati erano soggetti a misure di protezione tali da renderli incomprensibili, perché per es. sottoposti a cifratura;
– 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;
– la comunicazione *ad personam* richiederebbe sforzi sproporzionati per l'elevato numero di interessati. In tal caso, il Comune può procedere ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia; es. tramite web o giornale locale.

### Art. 35 - Documentazione della violazione - Registro della violazione

1. Il Titolare del trattamento documenta ogni violazione dei dati personali, anche quelle che non vengono notificate al Garante nè comunicate agli interessati, la procedura avviata internamente all'ente locale ed i provvedimenti per porvi rimedio. A tal fine redige apposita scheda tecnica cui sono allegati le relazioni degli autorizzati al trattamento ed il parere del RPD.
2. Il Titolare del trattamento annota la violazione nel Registro delle violazioni, che contiene tra le altre informazioni: l'ufficio dell'ente locale competente al trattamento dei dati violati, la descrizione e la gravità del *data breach*, l'indicazione dei dispositivi cartacei o automatizzati coinvolti, la categoria dei dati violati e dei destinatari, le misure di sicurezza presenti ed applicate ai dati violati e le ulteriori eventuali misure adottate.
3. La documentazione è a disposizione di eventuali ispezioni e verifiche da parte del Garante privacy.

## TITOLO VII

## ENTRATA IN VIGORE

### Art. 36 - Abrogazioni

1. Il presente Regolamento sostituisce il Regolamento sui dati sensibili, adottato prima dell'entrata in vigore del Regolamento UE 679/2016 ed approvato, ferme restando le schede/tabelle allegate allo stesso, che identificano i dati sensibili e giudiziari rispetto ai quali è consentito il trattamento, nonché le attività di trattamento consentite tenuto conto delle specifiche finalità di rilevante interesse pubblico perseguite nei singoli casi ed espressamente elencate dalla legge, le quali continuano ad applicarsi e sono altresì allegate al presente Regolamento per farne parte integrante e sostanziale. Per quanto non previsto nel presente Regolamento si applicano direttamente le norme del Regolamento UE 679/2016.
2. Il presente Regolamento fa riferimento alle sole norme del Codice della privacy, D.Lgs.196/2003, ancora oggi vigenti.

### Art. 37 - Entrata in vigore del Regolamento

1. Il presente Regolamento entra in vigore il giorno in cui diviene esecutiva la relativa delibera di approvazione.

2. Il presente Regolamento e la relativa modulistica per l'esercizio dei diritti da parte dell'interessato, sono resi pubblici mediante pubblicazione sul sito internet istituzionale dell'Ente, nella Sezione Amministrazione Trasparente.
3. Copia del presente Regolamento va inoltrata al Segretario Generale, al RPD, alle Posizioni Organizzative autorizzate di I livello del trattamento, agli autorizzati di II livello/incaricati ed ad ogni altro dipendente che tratta dati personali nel Comune.