



# COMUNE DI SASSETTA



## **REGOLAMENTO PER LA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI**

(Approvato con Deliberazione di Consiglio n. 21 del 31/07/2024 )



VISTI:

- IL REGOLAMENTO GENERALE PER LA PROTEZIONE DEI DATI PERSONALI 2016/679/2016/679 “GENERAL DATA PROTECTION REGULATION” O GDPR;
- LA NORMATIVA NAZIONALE DI CUI AL CODICE DELLA PRIVACY APPROVATO CON D.LGS 30 GIUGNO 2003, N. 196 COME SUCCESSIVAMENTE MODIFICATO DAL D.LGS 10 AGOSTO 2018, N. 101;
- DIRETTIVA UE 2019/1937 COME RECEPITA NEL D.LGS 10 MARZO 2023, N. 24 “ATTUAZIONE DELLA DIRETTIVA (UE) 2019/1937 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, DEL 23 OTTOBRE 2019, RIGUARDANTE LA PROTEZIONE DELLE PERSONE CHE SEGNALANO VIOLAZIONI DEL DIRITTO DELL’UNIONE E RECANTE DISPOSIZIONI RIGUARDANTI LA PROTEZIONE DELLE PERSONE CHE SEGNALANO VIOLAZIONI DELLE DISPOSIZIONI NORMATIVE NAZIONALI”.

PER TUTTO QUANTO NON PREVISTO E DISCIPLINATO DAL PRESENTE REGOLAMENTO TROVA APPLICAZIONE LA NORMATIVA VIGENTE IN MATERIA. LA NORMATIVA RICHIAMATA SI INTENDE COSÌ COME MODIFICATA ALLA DATA DI ENTRATA IN VIGORE DEL PRESENTE REGOLAMENTO.



# INDICE GENERALE

ART. 1 OGGETTO DEL REGOLAMENTO

ART. 2 DEFINIZIONI

ART. 3 FINALITÀ DEL TRATTAMENTO

ART. 4 INTERESSATO E TITOLARE DEL TRATTAMENTO DEI DATI

ART. 5 RESPONSABILE DEL TRATTAMENTO DEI DATI

ART. 6 RESPONSABILE DELLA PROTEZIONE DEI DATI

ART. 7 SICUREZZA DEL TRATTAMENTO

ART. 8 IL REGISTRO DELLE CATEGORIE DI ATTIVITÀ

ART. 9 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ART. 10 VIOLAZIONE DEI DATI PERSONALI E COMUNICAZIONE AL GARANTE

ART. 11 VIOLAZIONE DEI DATI PERSONALI E COMUNICAZIONE AGLI UTENTI

ART. 12 DIRITTI DELL'INTERESSATO

ART. 13 ESERCIZIO DEI DIRITTI DELL'INTERESSATO

ART. 14 PRIVACY E PROCEDURE SELETTIVE BANDITE DAL COMUNE DI SASSETTA



## Articolo 1

### Oggetto del regolamento

1. Il presente Regolamento ha per oggetto misure procedurali e regole di dettaglio da osservarsi ai fini di una migliore funzionalità e dell'adeguamento delle azioni del Comune di Sassetta al Regolamento Generale Protezione Dati n. 679 del 27 aprile 2016, di seguito indicato GDPR, e della normativa interna relativamente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e libera circolazione dei dati.

## Articolo 2

### Definizioni

1. Si riportano alcune definizioni chiave in ambito privacy:
2. Amministratore di sistema: il soggetto preposto alla gestione di sistemi informatici con i quali vengono effettuati Trattamenti di Dati Personali.
3. Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure attraverso il quale viene verificata la corretta Identità di un utente.
4. Autorità di controllo: si intende l'Autorità di cui all'art. 51 del Regolamento Europeo in Materia di Protezione dei Dati Personali – General Data Protection Regulation [GDPR, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016], ovvero una o più Autorità pubbliche indipendenti incaricate da uno Stato Membro di vigilare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali.
5. Banca dati: una banca dati è una raccolta di informazioni/dati, in forma cartacea o informatica, organizzati in modo strutturato e omogeneo, in modo da poter essere facilmente reperite, aggiornate e modificate attraverso l'utilizzo di apposite chiavi di ricerca.
6. Cancellazione sicura: eliminazione di dati presenti sul supporto elettronico con modalità che li rendano inintelligibili e non recuperabili.
7. Credenziali di autenticazione: i dati e i dispositivi, assegnati a un soggetto e a esso univocamente correlati, utilizzati per l'autenticazione informatica.
8. Danno: conseguenza pregiudizievole derivante dal concretizzarsi di una minaccia.
9. Data Breach: violazione della sicurezza che comporta, accidentalmente o volontariamente, la distruzione, perdita, alterazione, pubblicazione o accesso non autorizzato di dati personali trasmessi, conservati o in altro modo trattati.
10. Data Protection Officer o DPO: soggetto designato dal Titolare del trattamento in funzione delle sue qualità professionali al fine di informare e fornire consulenza al Titolare stesso nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla Normativa Privacy.
11. Dato anonimo: il dato che in origine, o a seguito di trattamento, non si riferisce a una persona fisica identificata o identificabile.
12. Dati appartenenti a particolari categorie: i dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti,



sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati generici, 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.

13. Dati giudiziari: i dati personali relativi a condanne penali e reati ai sensi dell'art. 10 del GDPR, nonché i dati idonei a rivelare provvedimenti di cui all'rt. 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli art.li 60 e 61 del C.P.P.
14. Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile. 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* e a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
15. Diffusione: la trasmissione di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
16. Informazione: trasmissione dei dati e l'insieme delle strutture che la consentono.
17. Interessato: la persona fisica identificata o identificabile mediante i dati personali trattati.
18. Minaccia: evento il cui concretizzarsi potrebbe arrecare danno ai beni dell'Ente.
19. Misure adeguate: l'insieme delle misure tecniche e organizzative volte a garantire la liceità del trattamento effettuato, anche con riferimento alla disponibilità, autenticità, integrità e la riservatezza dei dati personali conservati o trasmessi, individuate sulla base e in relazione ai rischi individuati rispetto ad una determinata attività di trattamento.
20. Normativa Privacy: complessivamente, il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, la normativa italiana di riferimento (in particolare, il D.Lgs. 196/2003, come modificato e integrato dal D.Lgs. 101/2018 di adeguamento, nonché le regole di condotta tecniche ad esso collegate e i Provvedimenti dell'Autorità Garante per la protezione dei dati personali applicabili al contesto).
21. Persone autorizzate al trattamento: le persone fisiche autorizzate dal Comune a compiere operazioni di trattamento dei dati personali, nell'ambito e sotto l'autorità del Comune stesso, in ottemperanza alle istruzioni ricevute mediante apposita nomina.
22. Responsabile del trattamento: la persona giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento, appositamente designata ai sensi e in conformità all'art. 28 del GDPR.
23. Rischio: possibilità che un evento non voluto e potenzialmente dannoso si verifichi, facendo venir meno la riservatezza e/o l'integrità e/o disponibilità dei dati personali e , quindi, mettendo a repentaglio la tutela dei diritti e le libertà delle persone fisiche.
24. Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati a alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
25. Titolare del trattamento o Titolare: 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.
26. 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 distribuzione.

### **Articolo 3**

#### **Finalità del trattamento**

1. I dati personali devono essere trattati lealmente e lecitamente, rilevati per finalità determinate, esplicite e legittime, devono essere adeguati, pertinenti e non eccedenti le finalità per le quali vengono trattati, sono esatti e, se necessario, aggiornati. Il Comune di Sassetta si impegna a porre in essere tutte le misure necessarie per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati e, successivamente trattati. I dati sono conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati ed, in seguito, trattati.
2. Il Comune di Sassetta tratta i dati personali per le seguenti finalità:
  - a) esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
  - b) adempimento di un compito legale al quale è soggetto Il Comune di Sassetta;
  - c) esecuzione di un contratto;
  - d) salvaguardia di interessi vitali dell'interessato o di altra persona fisica;
  - e) per specifiche finalità diverse da quelle analizzate nei punti precedenti purché sussista la base giuridica del consenso dell'interessato al trattamento dei dati personali.

### **Articolo 4**

#### **Interessato e Titolare del trattamento dei dati**

1. Interessato: con il termine "Interessato" si fa riferimento alla persona fisica resa identificata o identificabile dai Dati Personali trattati (a titolo esemplificativo e non esaustivo: dipendenti, candidati all'assunzione, visitatori, committenti, richiedenti servizi ecc.).
2. Titolare del trattamento: titolare del trattamento è il Comune di Sassetta, rappresentato dal Sindaco p.t. o da un suo delegato. Il Titolare è responsabile del trattamento dei dati personali detenuti in ragione delle sue attività istituzionali o in ottemperanza agli obblighi di legge, nello svolgimento di compiti di interesse pubblico o connesso all'esercizio di pubblici poteri, raccolti o meno in banche dati, automatizzate o cartacee, nel rispetto dei principi applicabili al trattamento di cui all'art. 5 del GDPR e di seguito esplicitati:
  - a) liceità, correttezza e trasparenza: trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
  - b) limitazione delle finalità: 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: adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) esattezza: 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;

e) limitazione della conservazione: conservati in 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 periodo più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;

f) integrità e riservatezza: i dati devono essere 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.

## **Articolo 5**

### **Responsabile del trattamento dei dati**

1. Il Responsabile del trattamento dei dati personali è il soggetto sterno che tratta i dati per conto del Comune di Sassetta, i suoi compiti/doveri sono definiti da un accordo nel quale sono indicati:
  - l'oggetto e la durata del trattamento dei dati;
  - la natura e le finalità del trattamento;
  - il tipo di dati personali e le categorie di soggetti interessati;
  - le istruzioni/restrizioni per qualsiasi trasferimenti di dati personali sia all'interno che all'esterno del Comune;
  - l'applicazione di misure di sicurezza adeguate;
  - i diritti del Titolare del trattamento;
  - gli obblighi del Responsabile del trattamento.
  
2. Si indicano, qui di seguito, i principali obblighi del Responsabile:
  - l'accesso ai dati è autorizzato limitatamente all'espletamento delle proprie funzioni, vige, a carico del Responsabile, il divieto di comunicazione o diffusione di qualunque dato senza la preventiva autorizzazione del Titolare;
  - il Titolare si impegna a comunicare ufficialmente al Responsabile qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati. Pertanto, il Responsabile e le persone da questi autorizzate al trattamento dovranno rimodulare la loro attività, in base alle sopracitate variazioni;
  - il Responsabile deve verificare che i dati trattati non siano accessibili a terzi non autorizzati durante l'operatività ordinaria e straordinaria;



- il Responsabile dovrà attenersi alle istruzioni del Titolare contenute all'interno dell'accordo o in modifiche ed integrazioni scritte successive, nell'ambito dello svolgimento dei servizi;
- il Responsabile segue precise istruzioni da parte del Titolare, per quanto attiene ai trattamenti dei dati personali effettuati, con particolare attenzione alle categorie di dati personali, ex art. 9 del GDPR, ed ai dati relativi a condanne penali e rati, ex art. 10 del GDPR, nonché ai dati il cui contenuto presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

Se ricorre a persone a persone autorizzate al trattamento o ad altri Responsabili del trattamento, il responsabile, contestualmente alla nomina e pervia autorizzazione scritta del Titolare, fornisce specifiche e dettagliate istruzioni in linea a quanto richiesto dal Titolare e dalle disposizioni normativa applicabili. In particolare, il Responsabile del trattamento verifica che le persone autorizzate e gli altri Responsabili applichino tutte le disposizioni, in materia di sicurezza relativa alla custodia delle passwords e che conservino in luogo sicuro i documenti contenenti i dati personali, di cui agli articoli 9 e 10 del GDPR.

Il Responsabile è tenuto altresì a vincolare le persone autorizzate e gli altri Responsabili ad un obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di collaborazione, nelle forme che ritenga opportune, purché idonee e adeguate allo scopo.

Nel rispetto dei principi di riservatezza, il Responsabile, a titolo non esaustivo, deve:

-raccogliere, registrare e conservare i dati, cartacei e/o informatici, oggetto di trattamento, avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

-eseguire qualsiasi altra operazione di trattamento nei limiti del mandato ricevuto e nel rispetto della normativa vigente;

-assicurarsi che le misure di sicurezza adottate siano adeguate ad evitare i rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;

-se necessario, adottare misure di sicurezza, quali la pseudonimizzazione e la cifratura dei dati personali, nonché la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento ed infine la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali, in caso di incidente fisico o tecnico;

-rispettare il divieto di comunicazione a terzi se non per ragioni strettamente legate all'incarico, o con espressa autorizzazione del Titolare o per obbligo di legge o dell'Autorità.

3. Il Responsabile del trattamento è tenuto, in caso di violazione dei dati personali (data breach), ad informare senza in giustificato ritardo, il Titolare del trattamento in modo da consentire allo stesso (titolare) di adempiere alla notifica alla Autorità di controllo.

## **Articolo 6**

### **Il Responsabile della protezione dei dati**

1. Il Responsabile della protezione dei dati (RPD e DPO) è nominato dal Titolare del trattamento, nel rispetto di quanto previsto dall'art. 39, par. 1 del GDPR, svolge i seguenti compiti:



- a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- b) sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione 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 del GDPR;
- d) cooperare con il Garante per la protezione dei dati personali;
- e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- f) tenere il registro unico delle attività di trattamento in collaborazione con i vari Responsabili del trattamento;

2. I compiti del Responsabile della Protezione dei Dati personali attengono all'insieme dei trattamenti di dati effettuati dal Comune di Sassetta.

## **Articolo 7**

### **Sicurezza del trattamento**

1. Il Comune di Sassetta e ciascun Responsabile mettono in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio per i diritti e le libertà delle persone fisiche.
2. Le misure tecniche ed organizzative da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione, la minimizzazione, la cifratura, la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano dati personali, la capacità diripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidenti fisico o tecnico.

## **Articolo 8**

### **Il registro delle categorie di attività**

1. Ai sensi dell'art.30, paragrafi 1 e 2, del GDPR, è istituito il Registro delle attività di trattamento e delle categorie di trattamento;



2. ogni titolare del trattamento e, ove applicabile, il suo rappresentate tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene le seguenti informazioni:
  - il nome e i dati di contatto del Titolare del trattamento;
  - le finalità del trattamento;
  - una descrizione delle categorie di interessati e delle categorie di dati personali;
  - le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, inclusi i destinatari di Paesi terzi o di organizzazioni internazionali;
  - l'eventuale trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali;
  - ove applicabile, i termini previsti per la cancellazione delle diverse categorie di dati;
  - ove applicabile, una descrizione generale delle misure di sicurezza tecniche e organizzative del trattamento.
3. Ai sensi dell'art. 30, par. 2, GDPR ogni Responsabile del trattamento cura la tenuta del Registro delle attività di trattamento svolte per conto del Titolare, tale registro deve contenere:
  - il nome e i dati di contatto del Titolare del trattamento;
  - le categorie di trattamento effettuate per conto del titolare;
  - ove applicabile, i trasferimenti di dati verso un paese terzo o organizzazione internazionale;
  - ove applicabile, una descrizione generale delle misure di sicurezza tecniche e organizzative del trattamento.
4. I registri sono aggiornati tempestivamente in occasione delle variazioni dei trattamenti.

## **Articolo 9**

### **Valutazione di impatto sulla protezione dei dati**

1. Quando, per una tipologia di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, rincorrono le condizioni di cui all'art. 35 del GDPR che conducano alla necessità di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, tale valutazione dovrà essere effettuata dal Titolare del Trattamento, previa consultazione con il DPO il quale ultimo esprimerà un suo parere.
2. La Valutazione di impatto deve contenere almeno:
  - una descrizione sintetica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
  - una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
  - una valutazione dei rischi, incluse le garanzie, le misure di sicurezza ed 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 di altri soggetti.

## **Articolo 10**

### **Violazione dei dati personali e comunicazione al Garante per la protezione dei dati personali**



1. Per violazione dei dati personali (c.d. data breach) si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali detenuti, trasmessi, o, comunque, trattati dal Comune di Sassetta.
2. Se la violazione ha interessato il Responsabile del Trattamento, questo dovrà comunicare al Titolare e al DPO la violazione dei dati personali tempestivamente dall'avvenuta conoscenza della stessa, fornendo i dati informativi di cui al successivo comma 3 lettere a), c) e d) e qualora ritenga probabile che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, propone al Titolare la notifica della violazione al Garante per la protezione dei dati personali, ove possibile, entro settantadue ore dalla conoscenza. In caso di mancato rispetto del termine di settantadue ore, la notifica è corredata dai motivi di ritardo.
3. La notifica, ai sensi dell'art. 33 GDPR, deve contenere almeno:
  - a) una descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo delle registrazioni dei dati personali in questione;
  - b) il nome e i dati di contatto del DPO al fine di ottenere più informazioni;
  - c) una descrizione delle possibili conseguenze della violazione dei dati personali;
  - d) una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi;
4. Ai sensi dell'art. 33, comma 4, GDPR, qualora e nelle misure in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il Titolare del Trattamento documenta, a mezzo di apposito registro degli eventi, (registro dei data breach) qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

## **Articolo 11**

### **Violazione dei dati personali e comunicazione agli interessati**

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (interessati), il Titolare del trattamento comunica immediatamente la violazione all'interessato.
2. I principali rischi per i diritti e le libertà degli interessati conseguenti a una violazione sono:
  - a) danni fisici, materiali o immateriali alle persone fisiche;
  - b) perdita del controllo dei dati personali;
  - c) limitazione dei diritti e discriminazione;
  - d) furto o usurpazione di identità;



- e) perdite finanziarie, danno economico e sociale;
  - f) decifrazione non autorizzata, della pseudonimizzazione;
  - g) pregiudizio alla reputazione;
  - h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari e giudiziari).
3. La comunicazione, formulata in un linguaggio semplice e chiaro, deve contenere almeno le seguenti informazioni:
- a) il nominativo e i dati di contatto del DPO;
  - b) una descrizione delle probabili conseguenze violazioni dei dati personali;
  - c) una descrizione delle misure adottate, o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e, nel caso, attenuarne gli effetti negativi.
4. Nel caso in cui sussistano le seguenti condizioni, la comunicazione all'interessato non è richiesta:
- a) il Titolare del trattamento ha messo in atto tutte le misure tecniche e organizzative adeguate di protezione e tali misure erano state correttamente applicate ai dati personali oggetto della violazione;
  - b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio e, nel caso, attenuare gli effetti negativi;
  - c) per l'elevato numero di interessati, la comunicazione richiedere sforzi sproporzionati e, in tal caso, si può procedere con una comunicazione pubblica o simile, mediante la quale tutti gli interessati siano informati in modo uguale ed efficace.

## **Articolo 12**

### **I diritti dell'interessato**

1. Il Comune di Sassetta garantisce che i dati raccolti siano completi, accurati e mantenuti aggiornati rispetto al proposito per cui vengono raccolti, compatibilmente con le tempistiche necessarie per gli aggiornamenti e tenuto conto del numero di dati oggetto del trattamento.
2. I dati personali sono raccolti dal Comune di Sassetta per finalità specifiche solo per finalità lecite, legittime e specifiche.
3. Gli interessati, in relazione ai propri dati personali trattati dal Comune di Sassetta, hanno facoltà di esercitare i seguenti diritti:



- a) diritto di accesso: ovvero il diritto di ottenere conferma che sia o meno in corso un trattamento di dati che li riguardano e, in tale ultimo caso, di ottenere l'accesso ai dati personali, ottenere copia e ricevere informazioni;
- b) diritto di rettifica: ovvero il diritto di ottenere la rettifica dei dati inesatti che lo riguardano o l'integrazione dei dati incompleti;
- c) diritto alla cancellazione (diritto all'oblio): ovvero il diritto di ottenere la cancellazione dei dati che lo riguardano, se sussiste uno dei motivi sanciti dall'art. 17 GDPR;
- d) diritto alla portabilità dei dati: ovvero il diritto, nei casi previsti dall'art. 20 GDPR (trattamento effettuato con mezzi automatizzati basato sul consenso o sull'esecuzione di un contratto), di ricevere, in formato strutturato, di uso comune e leggibile da dispositivo automatico i dati che lo riguardano, nonché di trasmettere tali dati ad altro titolare del trattamento senza alcun impedimento. L'esercizio di tale tipologia di diritto non si applica all'ipotesi in cui il trattamento si fonda su interesse pubblico o interesse legittimo del titolare;
- e) diritto di limitazione del trattamento: ovvero il diritto di ottenere, nei casi indicati dall'art. 18 GDPR, la cancellazione/pseudonimizzazione/anonimizzazione dei dati personali che lo riguardano con l'obiettivo di limitarne il trattamento;
- f) diritto ad ottenere un processo decisionale non completamente automatizzato: ovvero il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla persona.

### **Articolo 13**

#### **Esercizio dei diritti da parte dell'interessato**

1. Per tutti i diritti il termine di risposta è un mese, estendibile a tre mesi in casi di particolare complessità. Il Titolare deve comunque dare riscontro all'interessato entro un mese dalla sua richiesta, anche in caso di diniego.
2. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Spetta al Titolare valutare la complessità del riscontro dell'interessato e stabilire, eventualmente, l'ammontare del contributo da richiedere, ma solo nel caso in cui si tratti di richiesta manifestamente infondata, eccessive o anche ripetitive, o se non chieste più copie nel caso di diritto di accesso. In questo ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti.
3. Il riscontro all'interessato deve avvenire, di regola, in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità. Può essere dato oralmente solo se lo richiede lo stesso interessato.
4. Per quanto attiene le limitazioni all'esercizio dei diritti dell'interessato si fa riferimento, altresì, a quanto aggiornato dall'art. 13, comma 3, della Direttiva 2019/1937.

### **Articolo 14**

#### **Privacy e procedure selettive bandite dal Comune di Sassetta**



1. I dati forniti dai candidati per la partecipazione alle procedure selettive vengono raccolti e trattati dal Servizio Personale e organizzato dal Comune di Sassetta per verificare la sussistenza dei requisiti richiesti ai fini dell'ammissione dei titoli dichiarati.
2. I dati forniti dai candidati vengono acquisiti per i fini connessi alla procedura selettiva e sono classificati come: dati personali comune (es. anagrafici e di contatto), dati relativi a condanne penali e a reati (c.d. dati giudiziari); categorie particolari di dati (c.d. dati sensibili) nei quali ultimi vanno annoverati anche i dati necessari a fornire adeguato supporto ai candidati con disabilità e necessari alla verifica dei requisiti personali dichiarati.
3. I dati potranno essere trattati dal Servizio Personale e organizzazione che cura il procedimento di selezione, da personale di altri servizi dell'ente che svolgeranno attività connesse (ad e. ufficio protocollo), nonché dai soggetti esterni, limitatamente alle fasi della selezione rimesse alla loro supervisione, così come da convenzioni che il Comune di Sassetta stipulerà. I dati così trattati verranno comunicati ai soggetti che facciano richiesta di accesso ai documenti di selezione, nei limiti consentiti dalla normativa vigente, e alle Autorità competenti.
4. Per quanto, in ultimo, concerne le graduatorie e gli esiti delle prove dei concorsi banditi dal Comune di Sassetta, la scrivente amministrazione applica la c.d. pseudonimizzazione del dato. Attraverso questa modalità di trattamento dei dati personali non possano più essere attribuiti a un interesse specifico senza l'utilizzo di informazioni aggiuntive. Tali informazioni aggiuntive sono conservate separatamente dal Servizio Personale e organizzazione e soggette a misure tecniche e organizzative intese a garantire che tali dati siano attribuiti a una persona fisica identificata o identificabile.
5. Nell'ipotesi in cui il Comune di Sassetta decida di affidare ad un soggetto esterno la gestione di talune o di tutte le fasi delle procedure selettive bandite, verrà stipulata convenzione nella quale verranno regolati gli aspetti al trattamento dei dati personali dei candidati nonché della nomina del responsabile del trattamento.