Allegato A)

UNIONE DI COMUNI VERONA EST

(Provincia di VERONA)

Manuale di organizzazione per l'attuazione della disciplina sulla protezione dei dati personali

(MANUALE PRIVACY)

Approvato con deliberazione di Giunta Unione n. _____del ____

Note: le sigle (C...) nell'articolato del presente regolamento si riferiscono ai "Considerando" del Reg. UE679/2016

Sommario

PREMESSE

Il presente manuale fornisce nella forma di un regolamento organizzativo, il quadro ricognitivo delle disposizioni di rango primario – a partire dal Reg. UE 679/2016 - e secondario per l'attuazione delle misure per la protezione dei dati personali trattati dall'Amministrazione Comunale in ragione delle proprie competenze ed attribuzioni. Nell'articolato, il richiamo alla fonte non è sempre esplicitato. È chiaro, tuttavia, che tale ricognizione non ha – e non può avere – nessuna valenza novativa rispetto alle fonti di rango superiore.
Oltre alla contestualizzazione normativa, che si è ritenuto utile collettare in una sorta di codice ad uso interno per un più pronto riferimento, si sono affrontati gli aspetti organizzativi, fornendo agli operatori dell'Amministrazione le linee di indirizzo generali nella gestione dei dati personali. Di particolare importanza, nell'ambito dell'organizzazione, è il CAPO V che individua appunto l'ORGANIGRAMMA PRIVACY.

CAPO I DISPOSIZIONI GENERALI

Articolo 1. **Definizioni**

Al fine del presente regolamento valgono le seguenti definizioni:
1) **«dato personale»:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (C26, C27, C30)
2) **«trattamento»:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) **«limitazione di trattamento»:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)
4) **«profilazione»:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)
5) **«pseudonimizzazione»:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)
6) **«archivio»:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (C15)

7) **«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; (C74)
8) **«responsabile del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio oaltro organismo che tratta dati personali per conto del titolare del trattamento;
9) **«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; (C31)
10) **«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;
11) **«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; (C32, C33)
12) **«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'accessoai dati personali trasmessi, conservati o comunque trattati; (C85)
13) **«dati genetici»:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della personafisica in questione; (C34)
14) **«dati biometrici»:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (C51)
15) **«dati relativi alla salute»:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (C35)
16) **«stabilimento principale»:** (C36, C37) a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
17) **«rappresentante»:** la persona fisica o giuridica stabilita nell'Unione che, designata dal

titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento; (C80)

18) **«impresa»:** la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
19) **«gruppo imprenditoriale»:** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate; (C37, C48)
20) **«norme vincolanti d'impresa»:** le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; (C37, C110)
21) **«autorità di controllo»:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
22) **«autorità di controllo interessata»:** un'autorità di controllo interessata dal trattamento di dati personali in quanto: (C124) a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;
23) **«trattamento transfrontaliero»:** a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
24) **«obiezione pertinente e motivata»:** un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
25) **«servizio della società dell'informazione»:** il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
26) **«organizzazione internazionale»:** un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Articolo 2. **Finalità del presente regolamento e competenza per l'approvazione**

Il presente regolamento:

a) ha funzioni ricognitiva del quadro normativo che regola la materia, organizzandola in una fonte normativa secondaria. Si disapplica laddove per l'evoluzione successiva del quadro regolatorio comunitario ed interno, lo stesso contrasti con le fonti di rango superiore ovvero con provvedimenti dell'Autorità Garante della Protezione dei Dati Personali (d'ora in poi, Garante);
b) disciplina gli aspetti organizzativi interni in tema di gestione dei dati personali. Fornisce

altresì le linee di indirizzo generali nella gestione dei dati personali e può pertanto essere considerato contemporaneamente atto generale di organizzazione e “istruzione dettagliate” per i designati al trattamento dei dati.

È pertanto attribuita alla Giunta, ai sensi dell’art. 48 comma 3 del TUEL, la competenza all’approvazione del presente regolamento.

Articolo 3. **Ambito oggettivo di applicazione del Regolamento UE 679/2016**

Il Regolamento UE 679/2016, d’ora in poi anche GDPR, si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Il GDPR non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (C18);

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98. 4. Il GDPR non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

Per il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati si applica la direttiva 2016/680 recepita in Italia con il decreto legislativo 18 maggio 2018, n. 51.

CAPO II PRINCIPI

Articolo 4. **Principi generali e responsabilizzazione**

L’Unione di Comuni Verona Est dà attuazione ai principi generali sanciti dal GDPR in tema di trattamento dei dati personali, per effetto dei quali i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principio di liceità, correttezza e trasparenza);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati modo che non vi sia incompatibilità 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 (principio della limitazione della finalità);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");

d) esatti e, se necessario, aggiornati, pertanto devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (principio di "esattezza");

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo

non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato (principio della "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 (principio di "integrità e riservatezza");
g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità (principio di necessità).
Il titolare adotta tutte le azioni necessarie al rispetto dei principi sopra declinati, e deve essere in grado di comprovarlo (principio di "responsabilizzazione" accountability).

Articolo 5. **Liceità del trattamento dei dati**

In ordine al principio di liceità del trattamento (art. 6 GDPR) il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto Titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
Essendo il titolare un'autorità pubblica, la lettera f) [legittimo interesse] non si applica al trattamento di dati effettuato nell'esecuzione dei propri compiti e funzioni.

Articolo 6. **Principio di finalità nel trattamento dei dati**

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

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del GDPR, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo GDPR;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 7. **Trattamento dei dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri**

Il trattamento dei dati effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, e quindi senza consenso dell'interessato, è possibile solo se il trattamento è previsto da una norma di legge o, nei casi previsti dalla legge, da regolamento.
La comunicazione fra titolari che effettuano trattamenti di dati personali diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento , e di quelli relativi a condanne penali e reati di cui all'articolo 10 del GDPR , per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, è ammessa se prevista da una norma di legge o di regolamento. In mancanza, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati .

Articolo 8. **Precisazioni sul consenso**

Fermi restando i casi nei quali il trattamento può essere legittimamente effettuato senza consenso, se il trattamento dei dati personali, per una o più specifiche finalità, è subordinato al consenso dell'interessato, si applica la disciplina del GDPR la quale prevede che:

a) qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
b) se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una dichiarazione che costituisca una violazione del GDPR è vincolante;
c) l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato deve essere informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato;
d) nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia stata condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto;

e) per i dati particolari previsti dall'articolo 9 del GDPR il consenso deve essere esplicito ed in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;
f) il consenso dei minori è valido a partire dai 14 anni; prima di tale limite di età previsto dalla normativa nazionale occorre raccogliere il consenso dei genitori o di chi ne fa le veci;
g) il consenso deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle prespuntate su un modulo);
h) il consenso deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.

La conservazione dei consensi è disciplinata dal manuale dei flussi documentali e dal manuale della conservazione dei documenti.

Articolo 9. **Informative**

Nel rispetto del principio di trasparenza, il titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste 13 e 14 del GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, ma può essere fornita anche oralmente, a condizione che si sia in grado di dimostrare di averla fornita (testimoni, registrazione vocale, etc.).

L'informativa può essere fornita, mediante:

a) pubblicazione sul sito web istituzionale di un'informativa generale sulle politiche del trattamento dei dati del titolare che preveda un rinvio al registro generale dei trattamenti, anch'esso pubblicato sul sito web istituzionale;
b) apposite comunicazioni, cartacee o digitali, consegnate al momento della raccolta dei dati, contenenti tutte le informazioni previste dagli articoli 13 e 14 del GDPR oppure un'informativa sintetica che rimandi all'informativa estesa pubblicata sul sito istituzionale dell'ente;
c) inserimento di apposita sezione all'interno dei bandi di gara, bandi di concorso, contratti, convenzioni, etc.

L'informativa relativa ai dati acquisiti direttamente presso l'interessato deve contenere almeno le seguenti informazioni:

a. *estremi identificativi e di contatto del titolare del trattamento e del rappresentante (ove designato)*
b. *dati di contatto del Responsabile della Protezione dei dati, d'ora in poi anche DPO*
c. *finalità, motivazioni giuridiche e modalità del trattamento*
d. *legittimi interessi perseguiti dal titolare del trattamento o da terzi*
e. *destinatari o categorie di destinatari ai quali i dati personali possono essere comunicati*

f. *eventuale trasferimento dei dati personali a un paese terzo o a un'organizzazione internazionale con indicazione delle eventuali garanzie privacy*
g. *periodo di conservazione dei dati personali o criteri utilizzati per determinare tale periodo*
h. *esistenza dei diritti di accesso, rettifica, cancellazione, limitazione, opposizione e portabilità*
i. *esistenza del diritto di revocare il consenso in qualsiasi momento*
j. *diritto di poter proporre reclamo a un'autorità di controllo privacy*
k. *natura obbligatoria o facoltativa del conferimento*
l. *conseguenze di un eventuale rifiuto a rispondere*
m. *esistenza di attività di profilazione o di processi decisionali automatizzati, logica utilizzata e conseguenze per l'interessati*

L'informativa relativa ai dati NON acquisiti direttamente presso l'interessato deve contenere almeno le seguenti informazioni:

a. *estremi identificativi e di contatto del titolare del trattamento e del rappresentante (ove designato)*
b. *dati di contatto del privacy officer (ove nominato)*
c. *finalità, motivazioni giuridiche e modalità del trattamento*
d. *legittimi interessi perseguiti dal titolare del trattamento o da terzi*
e. *destinatari o categorie di destinatari ai quali i dati personali possono essere comunicati*
f. *eventuale trasferimento dei dati personali a un paese terzo o a un'organizzazione internazionale con indicazione delle eventuali garanzie privacy*
g. *periodo di conservazione dei dati personali o criteri utilizzati per determinare tale periodo*
h. *esistenza dei diritti di accesso, rettifica, cancellazione, limitazione, opposizione e portabilità*
i. *esistenza del diritto di revocare il consenso in qualsiasi momento*
j. *diritto di poter proporre reclamo a un'autorità di controllo privacy*
k. *fonte da cui provengono*

Il titolare elabora le istruzioni ed un modello di informativa da fornire ai soggetti addetti al trattamento dei dati.

Articolo 10. **Formazione e sensibilizzazione**

In esecuzione all'articolo 29 del GDPR il titolare organizza appositi percorsi formativi continui ed obbligatori per il personale e per tutti coloro, anche rappresentanti politici, che abbiano accesso a dati personali.

CAPO III TRATTAMENTO DATI PERSONALI E REGISTRO DEI TRATTAMENTI

Articolo 11. **Dati personali**

11.1 Definizione

Il GDPR definisce "dato personale" [art. 4, n. 1, GDPR] "qualsiasi informazione concernente una persona fisica identificata o identificabile o la cui identità è manifestamente chiara o può essere facilmente accertata mediante l'ottenimento d'informazioni supplementari o ulteriori

ricerche".
Si considera identificabile la persona che può essere identificata, direttamente o indirettamente, mediante riferimento ad un nome, un numero di identificazione, un dato relativo all'ubicazione geografica, un codice identificativo online o ad uno o più specifici elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

11.2 Tipologia di dati personali
I dati personali sono classificati come segue:
a. dati personali comuni
b. dati personali particolari (ex sensibili)
c. dati giudiziari

11.2.1 Dati particolari
Sono considerati dati particolari quei dati personali idonei a rivelare:
- l'origine raziale od etnica;
- le convinzioni religiose, filosofiche o l'appartenenza sindacale;
- le opinioni politiche;
- i dati genetici, i dati biometrici intesi ad identificare in modo univoco una persona;
- i dati personali relativi alla salute o alla vita sessuale o all'orientamento sessuale.

11.2.2. Dati giudiziari
Il Regolamento non fornisce definizione puntuale di "dati giudiziari", ma fa rientrare in questa categoria tutti i dati personali relativi a condanne penali, reati o connesse misure di sicurezza [art. 10, GDPR].
Attualmente la normativa privacy italiana definisce "dati giudiziari" i dati personali idonei a rivelare provvedimenti in materia di:
a) casellario giudiziale;
b) anagrafe delle sanzioni amministrative dipendenti da reato e dei carichi pendenti;
c) qualità di imputato e di indagato.

Articolo 12. **Tipologie di trattamenti**

Il GDPR definisce "trattamento" [art. 4, n. 2, GDPR] qualunque operazione o complesso di operazioni, effettuate su un dato personale o su un insieme di dati personali, anche senza l'ausilio di strumenti elettronici o l'utilizzo di processi automatizzati.
I trattamenti, a titolo esemplificativo, possono essere classificati come segue
12.1 Raccolta
La raccolta dei dati è la prima operazione e generalmente rappresenta l'inizio del trattamento e consiste nell'attività di acquisizione del dato.
12.2 Registrazione
La registrazione consiste nella memorizzazione dei dati su un qualsiasi supporto.
12.3 Organizzazione
L'organizzazione consiste nella classificazione dei dati raccolti secondo un metodo prestabilito.
12.4 Strutturazione
La strutturazione consiste nell'attività di ripartizione dei dati secondi schemi prestabiliti.
12.5 Conservazione
La conservazione consiste nel mantenere memorizzate le informazioni su un qualsiasi supporto.
12.6 Adattamento (o modifica) ed elaborazione

L’adattamento o modifica consiste nell’attività di variazione del dato personale. L'elaborazione, invece, consiste nell'attività con la quale il dato personale subisce una modifica sostanziale.

12.7 Estrazione

L'estrazione consiste nell'attività di estrapolazione di dati da gruppi di dati già memorizzati.

12.8 Consultazione

La consultazione è l’operazione di lettura dei dati personali. Anche la semplice visualizzazione dei dati è un trattamento che può essere ricondotto nell'operazione di consultazione.

12.9 Uso o utilizzo

L’uso o utilizzo consiste in una generica attività che comprende qualsiasi tipo di impiego dei dati.

12.10 Comunicazione o cessione

La comunicazione (o cessione) consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, da titolare del trattamento, dal responsabile e da soggetti incaricati. In caso di comunicazione il dato viene trasferito a soggetti terzi, per tale motivo le attività di comunicazione o cessione di dati sono considerate particolarmente delicate.

12.11 Diffusione

Per diffusione, invece, si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, diffusione anche quando si pubblica online (es. pubblicazione di fotografie su un social network). In assenza di consenso tale attività deve ritenersi illecita.

12.12 Raffronto o interconnessione

Il raffronto è un'operazione di confronto tra dati, sia in conseguenza dell'elaborazione che della selezione o consultazione. L'interconnessione consiste nell'utilizzo di più banche dati, e presuppone l’impiego di strumenti elettronici.

12.13 Limitazione

La limitazione del trattamento è un contrassegno assegnato ai dati personali conservati con l’obiettivo di limitarne il trattamento futuro. La limitazione del trattamento dei dati personali deve essere chiaramente identificata e può essere assicurata mediante dispositivi tecnici in grado di garantire che i dati personali conservati non possano essere più sottoposti a ulteriori trattamenti o modificazioni.

12.14 Cancellazione o distruzione

La cancellazione consiste nell'eliminazione di dati tramite utilizzo di strumenti elettronici, mentre la distruzione è l'attività di eliminazione definitiva dei dati.

12.15 Profilazione

La profilazione è una qualsiasi forma di trattamento totalmente automatizzato di dati personali e consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica e, 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.

12.16 Selezione

La selezione consiste nell'individuazione di dati personali nell'ambito di gruppi di dati già memorizzati.

12.17 Blocco

Il blocco consiste nella conservazione dei dati con sospensione temporanea di ogni altra operazione di trattamento.

Articolo 13. **Trattamento dei dati particolari**

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le

convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Il trattamento dei dai particolari è permesso:

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

I trattamenti delle categorie particolari di dati personali per motivi di interesse pubblico (lettera g) comma precedente) sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di

regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
Fermo quanto previsto dal comma precedente si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

a) accesso a documenti amministrativi e accesso civico;
b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
c) tenuta di registri pubblici relativi a beni immobili o mobili;
d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale, comprese quelle di prevenzione e contrasto all'evasione fiscale;
j) attività di controllo e ispettive;
k) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
l) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;
m) rapporti tra i soggetti pubblici e gli enti del terzo settore;
n) obiezione di coscienza;
o) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
p) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
q) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
r) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;

s) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
t) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
u) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
v) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
w) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
x) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
y) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

13.1 Misure di garanzia del trattamento dei dati particolari

Le misure di garanzia per il trattamento dei dati particolari sono stabilite dal Garante con proprio provvedimento che viene adottato con cadenza almeno biennale.
È in ogni caso vietata la diffusione di dati relativi alla salute.
È ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, e dei provvedimenti del Garante.

Articolo 14. **Trattamento dati giudiziari**

Il trattamento dei dati giudiziari è lecito in quanto il titolare del trattamento è un’autorità pubblica.
Nel trattamento dei dati giudiziari devono essere rispettate le misure di sicurezza come previste dall’articolo 2 sexies del d.lgs 196/2003 e dalle linee guida del Garante.

Articolo 15. **Registro dei trattamenti**

L’Unione di Comuni Verona Est in qualità di titolare del trattamento tratta i dati personali per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari, nei limiti imposti dal Codice, dal GDPR, dalle Linee guida e dai provvedimenti del Garante.
Le attività di trattamento sono riportate in un “registro dei trattamenti” elaborato in base alle prescrizioni dell’articolo 30 del GDPR.
Il registro dei trattamenti deve contenere almeno le seguenti indicazioni minime:

a. *estremi identificativi e di contatto del titolare del trattamento (e degli eventuali contitolari o rappresentanti del trattamento);*
b. *estremi identificativi e di contatto del Data Protection Officer (DPO);*
c. *finalità del trattamento;*
d. *descrizione delle categorie dei soggetti interessati e descrizione delle categorie di dati personali trattati;*
e. *categorie di destinatari a cui i dati personali sono stati o saranno comunicati;*
f. *eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, con conseguente documentazione delle garanzie in materia di privacy;*
g. *ove possibile, il termine ultimo previsto per la cancellazione delle diverse categorie di dati (ove non è possibile indicare il termine di cancellazione i criteri utilizzati per determinare il termine ultimo di cancellazione);*
h. *descrizione generale delle misure di sicurezza tecniche e organizzative adottate.*

Il Registro dei trattamenti può altresì contenere qualsiasi altra informazione che il titolare ritenga utile indicare.

15.1 Approvazione del registro dei trattamenti

Il registro dei trattamenti è approvato con atto formale della Giunta Unione.

15.2 Aggiornamento del registro dei trattamenti

Il registro dei trattamenti va aggiornato annualmente attraverso l'approvazione annuale da parte della Giunta Unione. A tal fine (aggiornamento) ogni preposto al trattamento dei dati ha l'onere di aggiornare l'elenco dei trattamenti che riguardano la sua unità organizzativa.
In caso di attivazione di nuove attività di trattamento, cioè attività di trattamento non incluse nel registro dei trattamenti, il preposto interessato deve darne comunicazione al Referente privacy ed al Responsabile Protezione Dati, anche al fine di valutare la necessità di effettuare la DPIA (data protection impact assessment).
La gestione e l'aggiornamento del registro dei trattamenti è affidata al Responsabile dell'Area Affari Generali.
Il titolare emette ed approva apposite istruzioni per l'aggiornamento del registro dei trattamenti

15.3 Pubblicazione del registro dei trattamenti

Il registro dei trattamenti potrà essere pubblicato sul sito web dell'ente nella sezione dedicata alla privacy.

CAPO IV DIRITTI DEGLI INTERESSATI

Articolo 16. **Pubblicità e diffusione di dati personali in atti amministrativi**

Il Titolare, in sede di pubblicazione e diffusione, tramite l'albo pretorio informatico ed il sito web, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi: (a) sicurezza; (b) completezza; (c) esattezza; (d) accessibilità; (e) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.

Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, tranne deroghe previste da specifiche disposizioni.
Salva diversa disposizione di legge, il titolare garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on line o sul sito web dell'ente mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.
In ogni caso, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere sensibile o giudiziario dell'interessato, devono essere anonimizzati con adeguate tecniche di anonimizzazione.
I dati sensibili e giudiziari sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.
Il titolare si conforma alle linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.

Articolo 17. **Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali**

I presupposti, le modalità ed i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e per l'esercizio del diritto di accesso civico, semplice e generalizzato e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i dati sensibili e giudiziari.
Le attività finalizzate all'applicazione di tale disciplina [accesso agli atti] si considerano di rilevante interesse pubblico ai sensi dell'articolo 2 sexies del d. lgs 196/2003.
Il titolare si conforma alle linee guida dell'ANAC e del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

Articolo 18. **Diritti dell'interessato**

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

18.1 Diritto di accesso

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma se sia o meno in corso un trattamento di dati personali che lo riguardano, in tal caso ha diritto di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o ad un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.
Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.
Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune e formato aperto.
Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

18.2 Diritto alla rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
Il titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

18.3 Diritto alla cancellazione

Il diritto alla cancellazione o diritto "all'oblio", consistente nel diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo.
Il diritto alla cancellazione 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 GDPR;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

18.4 Diritto alla limitazione

L'interessato ha il diritto di ottenere dal titolare la limitazione del trattamento quando:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 GDPR, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare prima che detta limitazione sia revocata.
Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

18.5 Diritto alla portabilità

Il diritto alla portabilità dei dati consiste nel diritto a richiedere che i dati oggetto di trattamenti automatizzati compiuti dal titolare del trattamento siano trasmessi, senza impedimenti, o all'interessato stesso o ad altro titolare da lui indicato, utilizzando un formato "strutturato, di uso comune e leggibile da dispositivo automatico".
Il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

18.6 Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano per motivi di interesse pubblico o per l'esercizio di pubblici poteri nonché alla profilazione.
In caso di opposizione il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del GDPR, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Articolo 19. **Modalità di esercizio dei diritti dell'interessato**

Il Titolare pubblica sul sito web un indirizzo mail a cui gli interessati possono far pervenire le richieste di esercizio dei diritti di cui agli articoli precedenti ed il modulo per l'esercizio dei diritti.
La casella mail per l'esercizio dei diritti degli interessati è gestita dall'ufficio del Responsabile privacy // DPO.

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

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

La richiesta, per l'esercizio dei diritti di accesso ai dati personali, può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.
Fermo restando l'accesso ai dati personali, il responsabile privacy autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.
I soggetti competenti alla valutazione dell'istanza sono: (a) il responsabile privacy; (b) il preposto al trattamento dei dati competente
Le richieste di esercizio dei diritti degli interessati sono evase nel termine di 30 giorni. Il termine può essere prorogato di altri 30 giorni previa tempestiva comunicazione all'interessato.
In caso di mancato riscontro alle richieste entro 30 giorni l'interessato può richiedere l'intervento del Responsabile Protezione Dati (DPO).
Rimane ferma la possibilità di adire il Garante della Protezione dei dati ai sensi dell'articolo 77 del GDPR.
L'accesso dell'interessato ai propri dati personali può altresì essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.
Il titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Articolo 20. **Indagini difensive**

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

Articolo 21. **Limitazione all'esercizio dei diritti**

I diritti di cui agli articoli da 15 a 22 del GDPR, ai sensi dell'articolo 2 undecies del d.lgs. 196/2003, non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del GDPR qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;
f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio;
g) agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale

Nei casi di cui al comma 1, lettere a), b), d), e), f) e g) i diritti sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore.

L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d), e), f) e f-bis) 3 . In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facoltà di cui al presente comma.

CAPO V ORGANIGRAMMA PRIVACY – I SOGGETTI

Articolo 22. **Titolare del trattamento dati**

Titolare del trattamento dati è 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.

Titolare del trattamento è quindi l'Unione di Comuni Verona Est e le funzioni di titolare sono esercitate dal Presidente pro tempore in qualità di legale rappresentante ai sensi dell'articolo 50 del d.lgs. 267/2000.

Il Titolare del trattamento provvede a:

a) definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento dei dati personali, provvedendo alla definizione degli obiettivi strategici ed operativi nel DUP e negli altri documenti di programmazione e pianificazione;

b) mettere in atto misure tecniche e organizzative adeguate per garantire che i trattamenti siano effettuati in modo conforme al GDPR e alla norme in materia;
c) delegare e/o attribuire, con proprio atto, in tutto o in parte le funzioni ed i poteri del titolare di trattamento, a personale dell'ente adeguatamente formato ed istruito;
d) formare e aggiornare l'elenco dei soggetti designati al trattamento dei dati ed eventualmente pubblicarlo sul sito web istituzionale dell'ente;
e) istituire il ruolo organizzativo di "Responsabile privacy" all'interno dell'ente ed attribuirlo a personale adeguatamente formato ed istruito;
f) designare, con proprio atto, il Responsabile per la protezione dei dati personali (DPO) e/o fornire linee di indirizzo per l'affidamento del servizio all'esterno;
g) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
h) favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
i) favorire l'adesione a meccanismi di certificazione;
j) assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

Articolo 23. **Contitolare del trattamento dei dati**

Il titolare del trattamento si trova in rapporto di contitolarità con altri titolari quando le finalità e i mezzi del trattamento sono definiti di comune accordo fra le parti.
I contitolari, ai sensi dell'articolo 26 del GDPR, sono tenuti a determinare, in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.
L'accordo può designare un punto di contatto per gli interessati.
L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati.
Il contenuto essenziale dell'accordo è messo a disposizione degli interessati. Indipendentemente dalle disposizioni dell'accordo interno, gli interessati possono esercitare i propri diritti nei confronti di e contro ciascun Titolare del trattamento.

Articolo 24. **Responsabili del trattamento e sub responsabili**

Il titolare del trattamento può affidare a soggetti terzi il trattamento dei dati per suo conto

24.1 Definizione
Si definisce 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".

24.2 Caratteristiche del responsabile del trattamento
Per garantire che siano rispettate le prescrizioni del GDPR il titolare può affidare le attività di trattamento solo a responsabili che presentino garanzie sufficienti, in termini di conoscenza specialistica, affidabilità e risorse, e che mettano in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento.

24.3 Accordo fra titolare e responsabile di trattamento

L'esecuzione dei trattamenti da parte di un responsabile del trattamento deve essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento.

L'accordo deve essere stipulato in forma scritta o altro formato elettronico.

L'accordo può essere un atto autonomo oppure una sezione del contratto principale.

L'accordo è stipulato dal Preposto competente alla gestione del trattamento.

24.4 Contenuto dell'accordo

L'accordo, ai sensi dell'articolo 28 del GDPR, deve avere almeno i seguenti contenuti minimi:

a) materia disciplinata;
b) durata del trattamento;
c) la natura e la finalità del trattamento;
d) il tipo di dati personali trattati;
e) le categorie di interessati;
f) gli obblighi e i diritti del titolare del trattamento.

L'accordo deve inoltre prevedere che il responsabile del trattamento:

(i) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
(ii) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
(iii) adotti tutte le misure richieste (c.d. misure di sicurezza) dall'articolo 32 del GDPR;
(iv) ricorra ad altro responsabile del trattamento solo su consenso del titolare del trattamento e stipuli con il sub responsabile un accordo che abbia gli stessi contenuti dell'accordo fra titolare e responsabile principale;
(v) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR;
(vi) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
(vii) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
(viii) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del GDPR, consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;
(ix) informi immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

24.5 Responsabilità del Responsabile del trattamento

Nel caso di mancato rispetto delle disposizioni contenute nell'accordo e in caso di mancata comunicazione al titolare dell'atto di nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso il Titolare, il Responsabile del trattamento.

In caso di utilizzo dei dati per finalità diverse rispetto a quelle stabilite nell'accordo il Responsabile del trattamento diventa Titolare in proprio del trattamento.

Articolo 25. **Responsabile della protezione dei dati personali** ***(Data Protection Officer-RPD/DPO)***

Il Sindaco, in qualità di legale rappresentante del Titolare designa il Responsabile della protezione dei dati (d'ora in poi anche RPD o DPO) in caso di attribuzione del ruolo a soggetti interni all'Ente. La Giunta può, su proposta del Sindaco, fornire indirizzi al Responsabile della Transizione Digitale o al Referente Privacy per l'affidamento del servizio all'esterno.
Il RPD/DPO svolge i seguenti compiti:

a) informa e fornisce consulenze al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti in tema di protezione dei dati;
b) verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
c) fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
d) funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
e) funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

Al RPD/DPO possono essere affidati anche altri compiti / funzioni che non siano incompatibili con il ruolo e che non determinino conflitto di interessi.
Il RPD/DPO deve essere in possesso di (competenze):

a) una conoscenza specialistica della normativa e delle prassi di gestione dei dati personali;
b) un'adeguata conoscenza delle procedure e delle norme che regolano il funzionamento degli enti locali;
c) deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse.

Il RPD/DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
Il Titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.
Il DPO riporta direttamente al Titolare del trattamento (e quindi al Sindaco) e si interfaccia con il Responsabile della Transizione Digitale ed il Referente privacy.

Articolo 26. **Referente in materia di protezione dei dati (Referente Privacy)**

Il Referente in materia di protezione dei dati (Referente privacy) coincide con il Responsabile dell'Area Affari Generali o comunque con l'area cui competono funzioni amministrative nel caso di mutamenti nell'attuale organizzazione dell'Ente.
Il ruolo di Referente privacy può essere assegnato unicamente ad un soggetto che ricopra una posizione apicale con incarico di posizione organizzativa.
Al Referente privacy, con apposita nomina, è normalmente assegnato anche il ruolo di Responsabile della Transizione Digitale (RTD).
La gestione del ruolo di Referente privacy e/o di RTD potranno essere oggetto di gestione associata.
Spettano al Referente privacy, a titolo esemplificativo, i seguenti compiti, funzioni, poteri attribuiti/delegati dal sindaco:

a) proporre gli obiettivi strategici ed operativi per il costante adeguamento dell'organizzazione ai dettati del GDPR, alla normativa nazionale, alle regole deontologiche allegate al Codice Privacy ed alle linee guida del Garante, proponendo l'inserimento di tali obiettivi strategici e/o operativi nel DUP e negli altri documenti di programmazione e pianificazione del Titolare;
b) coordinare l'attività dei titolari di P.O. nello svolgimento delle funzioni e dei compiti in ordine ai processi, procedimenti, e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, fornendo ad essi le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
c) formare ed aggiornare l'elenco dei designati dal Titolare a trattare i dati personali e dei soggetti autorizzati ed eventualmente a pubblicarlo sul sito web istituzionale del Titolare;
d) gestire il procedimento di affidamento all'esterno del ruolo di DPO sulla base degli indirizzi stabiliti dal Sindaco o dalla Giunta Comunale;
e) effettuare, anche in collaborazione con il RTD ed il DPO, periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
f) favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
g) favorire l'adesione a meccanismi di certificazione;
h) gestire, unitamente al DPO, i contatti con gli interessati che intendono esercitare i diritti garantiti dal GDPR;
i) gestire, unitamente al DPO, i contatti con il Garante privacy.

Articolo 27. **Preposti al trattamento dei dati**

Il Titolare del trattamento conferisce al personale titolare dei ruoli organizzativi apicali o di unità organizzativa di massima dimensione il ruolo di "preposto al trattamento dei dati" (dell'unità organizzativa di cui è responsabile), d'ora in poi solo preposto, attribuendo almeno i sotto indicati compiti, funzioni, ed i correlati poteri.
La nomina dei "preposti" avviene con apposito provvedimento del sindaco pro tempore. Tale nomina può essere inserita anche nell'atto di attribuzione del ruolo organizzativo di vertice (posizione organizzativa con funzioni dirigenziali).
Il provvedimento di nomina a preposto deve contenere l'indicazione dei compiti e delle responsabilità che sono affidate con la nomina.
Il provvedimento di nomina a preposto comporterà l'attribuzione almeno dei seguenti compiti, funzioni, poteri e responsabilità:

a) trattare i dati personali su istruzione del Titolare del trattamento;
b) garantire che le persone addette o autorizzate al trattamento dei dati personali appartenenti all'unità organizzativa da questi diretta si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) garantire il tempestivo ed integrale rispetto dei doveri del Titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del GDPR;
d) osservare le disposizioni contenute negli atti generali di organizzazione dell'ente nonché le specifiche istruzioni impartite dal Titolare;

e) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute negli atti generali di organizzazione adottati dall'ente, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;
f) collaborare con il Titolare del trattamento nella predisposizione del documento di valutazione d'impatto sulla protezione dei dati e nella definizione del Registro delle attività di trattamento, in collaborazione con l'Amministratore/i di sistema e con le altre strutture competenti del Titolare;
g) curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno della struttura organizzativa diretta per l'applicazione del Codice, del GDPR, e degli altri atti di natura generale;
h) assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;
j) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Codice, dal GDPR e dal presente atto;
k) contribuire alle attività di verifica del rispetto del Codice, del GDPR e del presente atto, comprese le ispezioni realizzate dal Titolare o da un altro soggetto da questi incaricato;
l) curare la costituzione e l'aggiornamento degli archivi/banche dati di competenza, a solo titolo esemplificativo: (i) elenco dei contitolari, elenco dei responsabili dei trattamenti, elenco dei designati autorizzati con i relativi punti di contatto; (ii) elenco hardware e software in uso all'ente;
m) garantire l'aggiornamento della ricognizione dei trattamenti;
n) fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

Ciascun titolare di posizione organizzativa responsabile d'area nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, è obbligato a:

a) comunicare tempestivamente l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;
b) comunicare la cessazione dei contratti di appalto che comportano trattamento dei dati ed assicurarsi che l'ex responsabile abbia cancellato i dati;
c) collaborare con il Titolare nella redazione della valutazione d'impatto sulla protezione dei dati e nella consultazione preventiva;
d) predisporre le informative previste e verificarne il rispetto;
e) fornirele informazioni necessarie per l'aggiornamento del registro dei trattamenti;
f) designare gli addetti e gli autorizzati al trattamento, e fornire loro specifiche istruzioni;

g) rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
h) garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della struttura organizzativa del Titolare ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali responsabili del trattamento;
i) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Ciascun preposto risponde al Titolare del trattamento di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.
I preposti sono destinatari di interventi di formazione e di aggiornamento obbligatoria annuali.

Articolo 28. **Addetti al trattamento dei dati personali dipendenti del Titolare**

Gli “addetti al trattamento dei dati”, d’ora in poi solo addetti, sono le persone fisiche, di norma, dipendenti del Titolare del trattamento, designati dai “preposti” a svolgere le operazioni di trattamento dei dati personali di competenza dell’unità organizzativa in cui sono incardinati.
La designazione di addetto al trattamento dei dati personali è di competenza del preposto al trattamento dei dati dell’unità organizzativa di competenza che di norma è il dirigente o la posizione organizzativa responsabile dell’unità organizzativa.
La designazione è effettuata con determinazione del preposto e individua specificatamente i compiti spettanti all’addetto e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.
A prescindere dalla formale attribuzione dell’incarico di addetto o soggetto autorizzato, si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.
Per effetto di tale disposizione, ogni dipendente preposto ad un determinato ufficio/servizio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, è da considerare, "autorizzato" ai sensi dell'art. 2 - quaterdecies del Codice.
Gli addetti ricevono dai preposti idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attività sui dati affidate e gli adempimenti a cui sono tenuti.
Gli addetti collaborano con i preposti e con gli altri organi individuati dal Titolare segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo. In particolare, gli addetti devono assicurare che, nel corso del trattamento, i dati siano:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
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;
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità pel quali i dati sono trattati;
f) trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate,

da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

Gli addetti sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e/o dal preposto in base alle istruzioni ricevute o in base agli generali di organizzazione

Gli addetti dipendenti del Titolare sono destinatari degli interventi di formazione e di aggiornamento obbligatorio annuali.

Articolo 29. **Autorizzati al trattamento**

Gli “autorizzati al trattamento dei dati”, d’ora in poi solo autorizzati, sono generalmente soggetti a cui, di norma, è concesso effettuare solo alcune tipologie di trattamenti, generalmente consultazione o uso dei dati ma non inserimento o modifica delle banche dati e dei relativi dati personali.

Rientrano nel novero dei soggetti autorizzati anche gli amministratori comunali (assessori e consiglieri comunali).

La designazione di “autorizzato” al trattamento avviene con atto del legale rappresentante dell’ente o con atto del preposto competente e deve contenere le istruzioni e le modalità di espletamento delle operazioni di trattamento.

Gli autorizzati devono essere destinatari di interventi di formazione a meno che il soggetto che autorizza il trattamento (legale rappresentante o preposto) attesti l’adeguata competenza in tema di trattamento dei dati del soggetto autorizzato.

Articolo 30. **Amministratore di sistema**

Per "amministratori di sistema" si devono intendere quelle figure professionali (interne o esterne all’ente) che hanno il compito di provvedere alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti.

Gli Amministratori di sistema, a titolo esemplificativo, possono essere così classificati

- amministratori di dominio: si tratta degli Amministratori dei domini Active Directory interni ed esterni; rientrano in questa categoria i componenti dei gruppi “Domain Admins” e tutti coloro che, attraverso un meccanismo di delega, hanno la possibilità di agire su un sottoinsieme degli oggetti dei domini;
- amministratori di server: si tratta degli utenti che hanno diritti amministrativi su uno o più server; rientrano in questa categoria, a titolo esemplificativo, gli utenti appartenenti al gruppo “Administrators” di uno o più server Windows o gli utenti di uno o più server Linux che, attraverso il comando “sudo”, possono impersonare l’utente “root”;
- amministratori di basi di dati: rientrano in questa categoria gli utenti che hanno la possibilità di manipolare la struttura di uno o più database attraverso comandi di “Data Definition Language”;
- amministratori di apparati di rete: rientrano in questa categoria gli utenti che hanno la possibilità di accedere ad apparati di rete layer 2 o layer 3 e modificarne le configurazioni;
- amministratori di apparati di sicurezza: rientrano in questa categoria gli utenti che possono modificare le configurazioni di sistemi hardware o software dedicati alla sicurezza, quali ad esempio firewall, sistemi di intrusion prevention, web proxy e sistemi antivirus;

- amministratori di software complessi: rientrano in questa categoria gli utenti che possono agire sui software in uso (ad esempio il gestionale, il software per la fatturazione ecc.) ma che non hanno acceso a credenziali amministrative del server su cui operano;
- amministratori dei sistemi di backup: rientrano in questa categoria gli utenti che gestiscono ed implementano le operazioni di backup e che sovrintendono al loro corretto funzionamento.

Sulla scorta delle indicazioni ed in collaborazione con il Responsabile della Transizione Digitale agli Amministratori di sistema, in base alle diverse competenze assegnate, possono essere assegnati i seguenti compiti:

a) gestire il sistema informativo-informatico inteso come complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni personali, attenendosi anche alle disposizioni del Titolare in tema di sicurezza;
b) predisporre ed aggiornare un sistema di sicurezza informatico 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, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, misure che comprendono, tra le altre, se del caso:
    i. la pseudonimizzazione e la cifratura dei dati personali;
    ii. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
    iii. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
    iv. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
c) collaborare nella predisposizione del Piano protezione dati per la parte concernente il sistema informatico ed il trattamento informatico dei dati;
d) elaborare e tenere aggiornato un disciplinare tecnico da portare in approvazione al Titolare del trattamento in cui siano disciplinati le misure e le procedure di sicurezza aziendali in tema di gestione del sistema informativo-informatico;
e) elaborare e tenere aggiornato un disciplinare tecnico per la gestione della posta elettronica ed internet;
f) elaborare e tenere aggiornato un sistema di valutazione dei rischi;
g) cooperare nella predisposizione della Valutazione d'impatto sulla protezione dati ai sensi dell'articolo 35 del Regolamento (anche DPIA – data protection impact assessement);
h) collaborare con il titolare e gli altri ruoli dell'organigramma privacy in caso di Data Breach;
i) redigere una relazione annuale sull'attività svolta in modo da permetterne la verifica;
j) vigilare sugli interventi informatici effettuati sul sistema informativo-informatico dell'ente e sull'impianto di videosorveglianza effettuati da vari operatori esterni ed in caso di anomalie segnalarle al Referente / Coordinatore privacy ed al Responsabile Protezione Dati / DPO (Data Protection Officier);
k) coordinare assieme al Titolare, al Responsabile Protezione Dati ed al Referente / Coordinatore privacy le attività operative degli addetti ai trattamenti informatici nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico;

l) collaborare con il Titolare ed il DPO per l'attuazione delle prescrizioni impartite dal Garante;
m) comunicare prontamente al Titolare qualsiasi situazione di cui sia venuto a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali;
n) verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore installati nei dispositivi presenti nell'unità produttiva;
o) adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica), sistemi di elaborazione e sistemi di archiviazione elettronica da parte di tutte le persone qualificate amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
p) assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nel Disciplinare tecnico, e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i codici identificativi personali da assegnare agli incaricati del trattamento dati, svolgendo anche la funzione di custode delle copie delle credenziali;
q) procedere, più in particolare, alla disattivazione dei codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei codici identificativi personali per oltre 6 (sei) mesi;
r) adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza 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 in conformità allo stesso Disciplinare tecnico;
s) adottare tutti i provvedimenti e le azioni necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico (disaster recovery) degli stessi con copie di back-up, vigilando sulle procedure attivate in struttura. L'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
t) indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici;

I ruoli di amministratori di sistema possono essere assegnati ad uno o più dipendenti dell'ente oppure, in caso di mancanza di professionalità adeguate all'interno, possono essere affidati all'esterno attraverso uno o più contratti di prestazione di servizi nei quali vanno indicate le specifiche prestazioni a cui è tenuto il prestatore di servizi.
L'attività degli amministratori di sistema è coordinata dal Responsabile della Transizione Digitale (RTD) e potrà essere regolamentata da apposito disciplinare tecnico.

CAPO VI RISCHI E MISURE DI SICUREZZA

Articolo 31. **Rischio**

31.1 Definizione di rischio
Per “rischio” si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità.

31.2 Gestione del rischio
La "gestione del rischio” può essere definita come l’insieme delle attività volte a stimare i rischi derivanti dal trattamento di dati personali (in relazione ai diritti e alle libertà dei soggetti interessati) e alle successive misure di sicurezza adottate per rendere il rischio “accettabile”.

31.3 Valutazione del rischio
Il Regolamento UE 679/2016 prevede due distinti ambiti di valutazione del rischio:

a) la valutazione generale del rischio in tema di trattamento dei dati previsto dall’art. 32 Regolamento e riguarda il rischio e le conseguenze dell’alterazione dei dati “lato ente”;
b) la valutazione d’impatto sulla protezione dei dati previsto dall’articolo 35 (DPIA) che riguarda il rischio (di impatto e di danno) “lato interessati”;

La valutazione del rischio va effettuata sui seguenti parametri:

I. probabilità di accadimento;
II. impatto dell’evento in caso di accadimento (in termini di effetti sugli interessati).

Dalla combinazione dei due fattori (probabilità * impatto) si ricava il livello di rischio che, posizionato sulla scala di valutazione, determina l’accettabilità o meno del rischio. In caso di livelli di rischio “non accettabili” sarà necessario intervenire con adeguate misure di sicurezza.

31.4 Metodologia di valutazione del rischio
L’Ente adotta, approva ed implementa una metodologia per la valutazione del rischio su cui devono basarsi le valutazioni.

31.5 La valutazione di impatto sulla protezione dei dati – DPIA
La valutazione di impatto sulla protezione dei dati, d’ora in poi DPIA (Data Protection Impact Assessment) è un onere posto direttamente a carico del titolare del trattamento, tramite il quale viene effettuata l'analisi dei rischi derivanti dai trattamenti posti in essere ed ha come oggetto della valutazione l’impatto “lato soggetti interessati”.
La valutazione di impatto, da realizzare per ogni singolo trattamento (o gruppi di trattamenti simili che presentano rischi analoghi), dovrà portare il titolare a decidere in autonomia se sussistono rischi elevati inerenti al trattamento; se sussistono rischi per i diritti e le libertà e degli interessati; se sarà necessario individuare le misure di sicurezza (tecniche ed organizzative) utili ad attenuare o eliminare tali rischi.
Al termine delle attività di valutazione di impatto sulla protezione dei dati personali, il titolare del trattamento deve redigere una relazione che deve almeno contenere:

- la descrizione sistematica dei trattamenti previsti;
- la finalità del trattamento, compreso l'interesse legittimo perseguito dal titolare;
- la valutazione dei principi di necessità e proporzionalità del trattamento, in relazione alla finalità perseguita;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento.

Sono obbligatoriamente sottoposte a DPIA le seguenti tipologie di trattamento:

a) Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso “app”, relativi ad “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”.
b) Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).
c) Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
d) Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
e) Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
f) Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
g) Trattamenti effettuati attraverso l’uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
h) Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
i) Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l’incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
j) Trattamenti di categorie particolari di dati ai sensi dell’art. 9 oppure di dati relativi a condanne penali e a reati di cui all’art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
k) Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.
l) Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.

Nel caso in cui la valutazione di impatto rilevi un rischio elevato che non può essere attenuato o eliminato dal titolare del trattamento mediante l'adozione di idonee contromisure (es. a causa degli elevati costi di attuazione o per indisponibilità tecnologica, etc.), il titolare è tenuto a consultare preventivamente [art. 36 del GDPR] l'Autorità di controllo (Garante Privacy Nazionale), prima di porre in essere il trattamento stesso.
L'ente adotta, approva ed implementa una metodologia per l'effettuazione della DPIA.

Articolo 32. **Misure di sicurezza**

Il titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate e misure di sicurezza che consentano di ridurre al minimo i rischi di alterazione dei dati personali trattati o di utilizzo non conforme alla finalità della raccolta.
In particolare, il titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate a garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono almeno:

a) la pseudonimizzazione e la cifratura dei dati personali trattati;
b) procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) modalità per garantire il ripristino tempestivo nell'accesso ai 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.

Per quanto attiene al trattamento dei dati personali effettuato con strumenti elettronici e non, il titolare applica le misure minime individuate da AGID.
L'Ente adotta un piano delle misure di sicurezza coordinato con il piano della sicurezza documentale.

CAPO VI AUTORITA' DI CONTROLLO

Articolo 33. **Autorità di controllo**

L'Autorità di controllo italiana è il Garante per la protezione dei dati personali.
I poteri dell'Autorità di controllo italiana sono stabiliti dall'articolo 58 del GDPR e dal Titolo II del codice privacy (d.lgs 196/2003) articoli 153 e seguenti.