Regolamento per l'applicazione del RGPD (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e del Codice Nazionale sulla Privacy dlgs 196/2003

Considerato che si rende necessario provvedere ad approvare il regolamento in oggetto , onde rispettare pedissequamente la normativa in materia ;

Ritenuto di poter provvedere in merito mediante l'approvazione dell'allegato atto di cui si condividono contenuti e finalità;

Visti :

il D.Lvo 267/2000;

lo Statuto ;

il GDPR 679/2016

il vigente Regolamento per il funzionamento degli Uffici e dei Servizi;

il parere favorevole alla regolarità tecnica reso dal responsabile del servizio ex art 49 del d.lgs 267/2000;

Con voti unanimi espressi nei modi di legge;

DELIBERA

1. di approvare l'allegato Regolamento .
2. di rendere il presente atto immediatamente eseguibile con separata ed unanime votazione ad hoc resa stante l'urgenza di provvedere in merito.

Regolamento per l'applicazione del RGPD (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e del Codice Nazionale sulla Privacy dlgs 196/2003

Sommario

Art. 1 - Oggetto del Regolamento

1. Il presente Regolamento disciplina le misure organizzative e le regole di dettaglio per la efficace attuazione da parte dell'Amministrazione del "General Data Protection Regulation (EU) 2016/679" (RGPD) ovvero "Regolamento generale sulla protezione dei dati" n. 679 del 27 aprile 2016 (di seguito indicato come RGPD), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali nonché alla libera circolazione di tali dati.

Art. 2 – Quadro normativo di riferimento

1. Il presente Regolamento tiene conto del seguente quadro normativo di riferimento:
   a) Codice in materia di dati personali (D.Lgs. n. 196/2003);
   b) Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. n.196 del 30 giugno 2003);
   c) Linee guida e raccomandazioni del Garante;
   d) RGPD del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
   e) Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del RGPD (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
   f) D.Lgs. n. 101/2018 di adeguamento della normativa interna al RGPD;
   g) Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) – 14/EN;
   h) Linee-guida sui responsabili della protezione dei dati (RPD) – WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   i) Linee-guida sul diritto alla "portabilità dei dati" – WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   j) Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento – WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
   k) Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 – WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
   l) Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative – WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;

m) Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione – WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
n) Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) – WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
o) Parere del WP29 sulla limitazione della finalità – 13/EN WP 203;
p) Norme internazionali;
q) Regolamenti interni dell'Ente.

Art. 3 – Definizioni

1. Il presente regolamento si avvale delle seguenti definizioni:
   - "Codice": D.Lgs. n. 196/2003;
   - "RGPD": Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;
   - "Regolamento": il presente Regolamento;
   - "Titolare": Amministrazione che adotta il presente Regolamento, sede istituzionale ;
   - "I designati al trattamento dei dati" (responsabili interni): i responsabili titolari di posizione organizzativa delle strutture di massima dimensione in cui si articola l'organizzazione dell'Ente, designati dal Legale rappresentante per l'esercizio di compiti e poteri in materia di trattamento dei dati personali.
2. Il presente regolamento recepisce le definizioni del D.Lgs. n. 196/2003 e del RGPD, fermo restando che, in caso di discordanza, prevalgono le definizioni contenute nei rispettivi testi normativi.

Art. 4–Finalità

1. L'Ente, nell'assolvimento delle proprie finalità istituzionali secondo i principi di trasparenza, efficacia ed economicità, garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.
2. Ai fini del presente Regolamento, per finalità istituzionali dell'Ente si intendono le funzioni ad esso attribuite dalle leggi, dallo statuto e dai regolamenti o per effetto di accordi e/o convenzioni.
3. I trattamenti di dati personali sono compiuti dall'Ente per le seguenti finalità:
   a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:
      - l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei

servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate all'Ente in base alla vigente legislazione.

b) l'adempimento di un obbligo legale al quale è soggetto l'Ente . La finalità del trattamento è in questo caso stabilita dalla fonte normativa che lo disciplina;
c) l'esecuzione di un contratto con i soggetti interessati;
d) le specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

4. In applicazione di quanto disposto dall'art. 25 del RGPD, i trattamenti di dati personali all'interno dell'Ente devono sottostare ai seguenti principi:
   - sin dall'inizio di una nuova tipologia di trattamento (fase di progettazione) la scelta delle modalità e dei mezzi utilizzati deve basarsi sulla necessità del rispetto della riservatezza e dei diritti fondamentali degli interessati ("privacy by design");
   - l'impostazione e l'organizzazione dei processi lavorativi deve costantemente sottostare a detta necessità, al fine di trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento ("privacy by default").
5. In adempimento dell'obbligo di comunicazione interna ed esterna, del rispetto degli obblighi di trasparenza e di semplificazione dell'azione amministrativa, l'Ente favorisce la trasmissione di dati e documenti tra le banche dati e gli archivi dell'Ente stesso, degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea, nell'ambito di specifiche disposizioni di legge o protocolli d'intesa.
6. La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità.
7. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi ed i procedimenti amministrativi di competenza del Titolare effettuati per lo svolgimento delle finalità istituzionali del medesimo, vanno gestiti conformemente alle disposizioni del Codice, del RGPD, del presente Regolamento e delle Linee Guida e dei provvedimenti del Garante.

Art. 5 – Principi e responsabilizzazione

1. Vengono integralmente recepiti, nell'ordinamento interno dell'Ente , i principi del RGPD, per effetto dei quali i dati personali sono:
   a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1 del RGPD, considerato incompatibile con le finalità iniziali ("limitazione della finalità");
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati in base al principio di "minimizzazione dei dati";
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati in base al 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 in base al principio di "limitazione della conservazione"; 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 del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dallo stesso regolamento a tutela dei diritti e delle libertà dell'interessato;
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 in base ai principi 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").

2. Il Titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di "responsabilizzazione".

Art. 6 – Liceità del trattamento

1. Vengono integralmente recepiti, nell'ordinamento interno del Titolare, le disposizioni del RGPD in odine alla liceità del trattamento e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
    a. l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
    b. il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
d. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e. il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
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.

2. La lettera f) di cui al comma precedente non si applica al trattamento di dati effettuato dal Titolare nell'esecuzione dei propri compiti e funzioni. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 del RGPD, 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:
   - di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
   - del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
   - della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo RGPD;
   - delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
   - dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art. 7 – Informativa

1. 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 dal RGPD e dall'art 13 del Codice, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
2. L'informativa è data per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online.
3. L'informativa è fornita, mediante idonei strumenti:
   a) Pubblicazione sul sito web dell'ente dell'informativa estesa, nella quale sono indicati anche i soggetti a cui l'utente può rivolgersi per ottenere

maggiori informazioni ed esercitare i propri diritti e le indicazioni sull'utilizzo dei cookie;
   b) attraverso appositi moduli da consegnare agli interessati;
   c) avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del Titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del Titolare;
   d) apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il Titolare.
4. L'informativa da fornire agli interessati può essere fornita anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.
5. Il Titolare garantisce all'interessato:
   a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
6. Nel fornire l'informativa, il Titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

Art. 8–Consenso dell'interessato

1. Il Titolare non deve richiedere agli interessati il consenso per il trattamento dei loro dati personali allorquando il trattamento dei dati è effettuato nello svolgimento dei propri compiti istituzionali di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito dal diritto dell'Unione o dello Stato.
2. Nelle fattispecie diverse da quelle di cui al precedente comma 1, qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
3. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
4. 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 prestato prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Art. 9 – Sensibilizzazione e formazione

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati e migliorare la qualità del servizio.
2. A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del Titolare e l'attività informativa diretta a tutti coloro che hanno rapporti con il Titolare.
3. Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.
4. Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.
5. La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene altresì integrata e coordinata con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Titolare.

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

1. Le disposizioni del presente Regolamento si intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno.
2. Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del Titolare, solo da parte dei soggetti appositamente autorizzati:

   - Titolare;
   - Designati al trattamento dei dati (responsabili delle strutture di massima dimensione in cui è articolata l'organizzazione dell'Ente);
   - Dipendenti, professionisti, collaboratori esterni e società fornitrici autorizzati al trattamento dei dati.
3. Non è consentito il trattamento da parte di persone non autorizzate.
4. L'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Ente, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale Ente provvede alla organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitare l'accesso e la fruizione, anche presso le strutture dipendenti.

5. Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale.
6. Il Titolare e tutti i soggetti coinvolti nel trattamento dei dati si attengono alle modalità di trattamento indicate nel Codice, nel RGPD, nonché nelle disposizioni attuative e nelle Linee guida del Garante per la protezione dei dati personali.

Art. 11 – Trattamento di categorie particolari di dati (così detti dati sensibili)

1. È vietato trattare, secondo quanto previsto dall'art. 9 del RGPD, 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.
2. Il divieto di cui al precedente comma non si applica se si verifica uno dei seguenti casi:

   a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al comma 1;

   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

   c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

   d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

   e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al successivo comma 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, del RGPD sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al comma 1 possono essere trattati per le finalità di cui al comma 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o dello Stato o alle norme stabilite dagli organismi nazionali competenti.

Art.12 – Trattamento dei dati sensibili e giudiziari

1. Il Titolare conforma il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.
2. A tale fine, il Titolare applica i principi degli articoli 20, 21 e 22 del Codice per il trattamento di dati sensibili e giudiziari, nonché le pertinenti disposizioni del RGPD, e si conforma alle Linee Guida del Garante in materia.

3. Il Titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati sensibili e giudiziari.

Art.13 - Trattamento dei dati sensibili relativi alla salute

1. Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali sensibili relativi allo stato di salute.
2. I dati idonei a rivelare lo stato di salute e la vita sessuale sono trattati da soggetti adeguatamente formati e sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

Art. - 14 Trattamento dei dati del personale

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

7. Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 15 - Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

1. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati sensibili e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.
2. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
3. Il Titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

Art. 16 – Diritti dell'interessato

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

Art. 17 – Diritto di accesso

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

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

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del RGPD, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.
3. 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 necessari. 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.
4. Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Art. 18 – Diritto alla rettifica e cancellazione

1. Il presente Regolamento tiene conto della disciplina del RGPD in tema di diritto di rettifica e cancellazione («diritto all'oblio»), di seguito indicata.
2. Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
3. 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.
4. Quanto al diritto "all'oblio", consistente nel diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:
   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 del RGPD;
   d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 del RGPD, 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.

Art. 19 – Diritto alla limitazione

1. Il presente Regolamento tiene conto della disciplina del RGPD in tema di diritto alla limitazione di seguito indicata.
2. L'interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:
   a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare per verificare l'esattezza di tali dati personali;
   b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
   c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del RGPD, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.
3. Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 del RGPD, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
4. L'interessato che ha ottenuto la limitazione del trattamento a norma del comma 1 è informato dal Titolare prima che detta limitazione sia revocata.
5. 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.
6. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 20 – Diritto alla portabilità

1. Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del RGPD, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Art. 21 – Diritto di opposizione e processo decisionale automatizzato relativo alle persone

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del RGPD, compresa la profilazione sulla base di tali disposizioni. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali per 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.

2. Il diritto di cui ai paragrafi 1 e 2 dell'art. 21 del RGPD è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
3. 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.
4. 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 RGPD, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Art.22 – Modalità di esercizio dei diritti dell'interessato

1. Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del RGPD, del Codice e del presente Regolamento.
2. 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.
3. 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.
4. L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.

5. Il soggetto competente alla valutazione dell'istanza è il Designato, ossia il responsabile in posizione apicale competente per materia, il quale decide sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.
6. All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa.
7. I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.
8. Il Titolare è tenuto a conformarsi alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Art. 23 - Titolare del trattamento

1. L'Ente , rappresentato ai fini previsti dal RGPD dal legale rappresentante pro-tempore, è l'autorità pubblica Titolare del trattamento dei dati ai sensi del RGPD ed esercita le proprie prerogative, poteri e doveri in ordine alle finalità ed ai mezzi del trattamento dei dati personali procedendo alla designazione e nomina: a) degli organismi/soggetti previsti dalla normativa e rimessi alla determinazione del Titolare nonché b) di eventuali gruppi di lavoro e/o team di progetto a supporto di specifiche attività.
2. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare definisce gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento ed è tenuto a mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali viene effettuato in modo conforme a quanto previsto dal RGPD.
3. Il Titolare definisce le misure fin dalla fase di progettazione e le mette in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
4. Nel caso in cui un tipo di trattamento, in particolare allorché questo prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una "valutazione dell'impatto del trattamento sulla protezione dei dati personali" (di seguito indicata con "DPIA": Data Protection Impact Assessment) ai sensi dell'art. 35 del RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 35.
5. Il Titolare provvede inoltre:
    - a nominare, con proprio atto, nelle persone del Segretario e dei responsabili delle singole strutture di massima dimensione in cui si articola l'organizzazione dell'Amministrazione (responsabili titolari di posizione organizzativa), i Designati al trattamento (Responsabili interni),

ai quali sono attribuiti compiti, funzioni e poteri in ordine ai processi, procedimenti e adempimenti relativi al trattamento dei dati personali contenuti nelle banche dati esistenti nelle articolazioni organizzative di competenza di ciascun Referente, alla sicurezza e alla formazione, impartendo ad essi le necessarie istruzioni in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;

- a nominare il Responsabile della protezione dei dati (RPD);
- a nominare i Responsabili (esterni) del trattamento;
- a pubblicare ed aggiornare, sul sito istituzionale dell'Ente , sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente, i propri dati di contatto e quelli del Responsabile della protezione dati;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
- ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.
- Tenere il registro unico dei trattamenti.

6. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'Amministrazione da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
7. L'Ente favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare, dei Referenti Responsabili e dei Responsabili esterni del trattamento.

Art. 24- Responsabile della protezione dati

1. Il Titolare, con suo provvedimento, nomina il DPO (Data Protection Officer), in seguito indicato con "RPD", Responsabile della protezione dei dati, sulla

base delle valutazioni economico-finanziarie ed organizzative deliberate con gli strumenti di programmazione annuale.

2. La nomina presuppone l'assenza di conflitto di interessi al fine di salvaguardare gli obblighi di indipendenza del RPD.
3. Il Responsabile della protezione dei dati è individuato in un soggetto esterno all'amministrazione, in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, all'adeguata conoscenza delle strutture organizzative degli Enti locali e delle norme e procedure amministrative agli stessi applicabili, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. I compiti attribuiti al RPD esterno sono indicati in apposito contratto di servizi o in alternativa nel decreto di nomina.
4. Il RPD esterno è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
5. E' possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione, nelle forme previste dal T.U. Enti Locali, approvato con D.lgs. 18.08.2000, n. 267 e s.m.i.
6. Il RPD è incaricato dei seguenti compiti:
   a) informare e fornire consulenza al Titolare ed ai Designati nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati personali. In tal senso il RPD può indicare al Titolare e/o ai Designati del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
   b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e dei Designati del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e dei Designati del trattamento;
   c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dai Designati;
   d) fornire, se richiesto, un parere scritto in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o

meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) fungere da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
f) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD ed i dati di contatto dello stesso devono essere pubblicati sul sito istituzionale e sono comunicati a cura del Titolare del trattamento al Garante della protezione dei dati personali. Allo scopo di garantire una supervisione da parte del vertice gestionale dell'Ente, le eventuali comunicazioni formali al Garante per la protezione dei dati personali sono sottoscritte anche dal Segretario generale;
g) la tenuta, qualora richiesto, dei registri di cui agli articoli 33 e 34;
h) altri compiti e funzioni, a condizione che il Titolare o i Designati del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

7. Il Responsabile della protezione dei dati deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   - il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
   - il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
   - il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente;
   - il RPD può convocare periodicamente riunioni di coordinamento dei Referenti del trattamento designati allo scopo di trattare questioni ritenute opportune per garantire la protezione dei dati personali.
8. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:
   a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
   b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed ai Referenti del trattamento interessati.
9. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Designati del trattamento;
- Qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

10. Da parte del Titolare e dei Designati, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente, devono essere garantite al RPD autonomia e risorse strumentali sufficienti per assolvere in modo efficace i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:
    - supporto attivo per lo svolgimento dei compiti da parte della Giunta e dei referenti interni, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;
    - supporto adeguato in termini di infrastrutture (sede, attrezzature, strumentazione);
    - comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
    - accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali;
    - posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.
11. Il RPD non può essere rimosso o penalizzato dal Titolare a causa dell'adempimento dei propri compiti.
12. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare e al Designato del trattamento competente per materia.
13. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare e al Designato interessato.
14. Il RPD mantiene uno stretto rapporto di collaborazione con il Segretario generale e con il responsabile del settore preposto alla gestione dei sistemi informativi.

Art. 25 – Designati a specifici compiti e funzioni connesse al trattamento dei dati (responsabili interni)

1. Il Titolare si avvale di più Designati al trattamento dei dati che presentino garanzie sufficienti per mettere in atto misure tecniche, organizzative e di sicurezza adeguate in modo tale che il trattamento dei dati personali

garantisca la tutela dei diritti dell'interessato nel rispetto del Codice, del RGPD e del presente Regolamento.

2. Allo scopo di cui al comma precedente ciascun dirigente ovvero responsabile titolare di posizione organizzativa delle strutture di massima dimensione in cui si articola l'organizzazione dell'Ente è nominato dal Sindaco, di norma, entro tre mesi dalla data della sua proclamazione, Designato a specifici compiti e funzioni connesse al trattamento dei dati. Sino a nuova designazione si intende prorogata di diritto la designazione degli stessi in carica al momento della predetta proclamazione.
3. La designazione dei Responsabili in posizioni apicali avviene con il decreto di attribuzione delle funzioni dirigenziali o con separato decreto, nel quale sono tassativamente previsti le seguenti funzioni e poteri:
   a) trattare i dati personali solo su istruzione del Titolare del trattamento e ai sensi di legge;
   b) assicurare, nell'esercizio dei compiti assegnati, il tempestivo ed integrale rispetto dei doveri del Titolare previsti dal Codice e dal RGPD;
   c) osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal Titolare;
   d) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;
   e) collaborare con il Titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione ed aggiornamento del Registro delle attività di trattamento, in collaborazione con l'Amministratore di sistema e con le altre strutture competenti del Titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
   f) curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del Titolare per l'applicazione del Codice, del RGPD, e del presente Regolamento;
   g) 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;
   h) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD (notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;

i) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, RGPD e nel presente Regolamento;
j) contribuire alle attività di verifica del rispetto del Codice, del RGPD e del presente regolamento, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato;
k) fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra l'Ente e ciascun Designato.

4. Ciascun Designato nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, collabora con il Titolare al fine di:
   - comunicare tempestivamente l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante al riguardo;
   - proporre eventuali autorizzati a specifici trattamenti di dati personali, e fornire loro specifiche istruzioni;
   - proporre la nomina dei responsabili (esterni) del trattamento dei dati nell'ambito degli appalti di servizi;
   - garantire la sensibilizzazione e l'aggiornamento del personale che partecipa ai trattamenti ed alle connesse attività di controllo, anche richiedendo al Titolare direttamente o tramite il RPD specifica attività di formazione;
   - 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;
   - garantire che tutte le misure, tecniche ed organizzative, di sicurezza del trattamento siano applicate all'interno della propria struttura ed all'esterno, qualora vi sia trattamento di dati personali afferenti le proprie competenze da parte di soggetti terzi quali Responsabili del trattamento;
   - informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.
5. I Designati Responsabili interni del trattamento sono destinatari di interventi di formazione e di aggiornamento.

Art. 26 – Autorizzati al trattamento

1. Gli autorizzati al trattamento sono i soggetti alle dipendenze dell'Ente addetti allo svolgimento di compiti e funzioni connessi al trattamento di dati personali di competenza nell'ambito delle mansion assegnate.

2. Gli autorizzati collaborano con il Titolare ed il Designato, Responsabile in posizione apicale, segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.
3. In particolare, gli autorizzati 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 per le 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.
4. Gli ~~autorizzati~~ sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal Designato nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del Titolare.
5. Gli autorizzati dipendenti del Titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 27 – Gli autorizzati al trattamento non dipendenti del Titolare

1. Tutti i soggetti che svolgono un'attività di trattamento dei dati, e che non sono dipendenti del Titolare, quali a titolo meramente esemplificativo i tirocinanti, i volontari, consulenti e i soggetti che operano temporaneamente all'interno della struttura organizzativa del Titolare così come gli incaricati nominati dai Responsabili del trattamento (esterni), devono essere autorizzati al trattamento tramite atto scritto di nomina o nell'ambito della disciplina contrattuale d'incarico.
2. Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli autorizzati dipendenti del Titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
3. Gli autorizzati non dipendenti dal Titolare possono essere comunque destinatari di interventi di formazione e di aggiornamento.

Art. 28 – Responsabili del trattamento (esterni)

1. Il Titolare su proposta dei Designati (responsabili interni) può nominare quali Responsabili esterni del trattamento di dati uno o più soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da tali soggetti esterni all'Ente in virtù di convenzioni, di contratti, di appalti, di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali. In tal caso il Titolare, ai sensi dell'art. 28 del RGPD, in considerazione della complessità e della molteplicità delle funzioni istituzionali, ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative, ivi compreso il profilo relativo alla sicurezza, adeguate in modo tale che il trattamento soddisfi i requisiti dello stesso RGPD e garantisca la tutela dei diritti dell'interessato.
2. Il Responsabile esterno è il soggetto che effettua un trattamento per conto del Titolare. Ove necessario per esigenze organizzative, possono essere nominati Responsabili più soggetti, anche mediante suddivisione di compiti.
3. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare.
4. Il trattamento di dati esternamente al Titolare da parte di un Responsabile del trattamento è disciplinato da un atto che regola il rapporto tra il Titolare ed il Responsabile del trattamento e deve in particolare stabilire quanto previsto dall'art. 28, comma 3, del RGPD; tale atto può anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
5. I Responsabili esterni del trattamento hanno l'obbligo di:
    a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto del Codice, del RGPD e del presente Regolamento;
    b) attenersi alle disposizioni impartite dal Titolare del trattamento;
    c) rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
    d) tenere per iscritto un registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare e che comprendono:
        - il nome e i dati del Titolare del trattamento per conto del quale opera, degli eventuali responsabili e del responsabile della protezione dei dati;
        - le categorie di trattamenti effettuati per conto del Titolare del trattamento;
        - se applicabili, i trasferimenti di dati a carattere personale verso un paese terzo o ad una organizzazione internazionale e, nel caso di trasferimenti previsti dall'articolo 49, paragrafo 1, secondo

comma del RGPD, i documenti che attestano l'esistenza di opportune garanzie;

e) nominare al proprio interno i soggetti autorizzati del trattamento;
f) garantire che i dati trattati siano portati a conoscenza soltanto del personale autorizzato del trattamento;
g) assistere il Titolare nella realizzazione di analisi di impatto relative alla protezione dei dati, conformemente all'articolo 35 del RGPD. Il Responsabile del trattamento assiste il Titolare nella consultazione preventiva dell'autorità di controllo, prevista dall'articolo 36 dello stesso RGPD;
h) adottare le misure adeguate di sicurezza necessarie per garantire la riservatezza e la protezione dei dati personali trattati;
i) specificare, se richiesti dal Titolare, le misure adottate di cui al punto precedente ed i luoghi dove fisicamente avviene il trattamento dei dati;
j) il Responsabile del trattamento notifica al Titolare ogni violazione di dati a carattere personale nel tempo massimo di 24 ore dopo esserne venuto a conoscenza, per via telefonica e pec. Tale notifica è accompagnata da ogni documentazione utile per permettere al Titolare, se necessario, di notificare questa violazione all'Autorità di controllo competente.

6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
7. Nel caso di mancato rispetto delle predette disposizioni, e in caso di mancata comunicazione al Titolare dell'atto di nomina di eventuali soggetti designati al trattamento dei dati, ne risponde direttamente, verso il Titolare, il Responsabile esterno del trattamento.

Art. 29 – Amministratore di sistema

1. L'Amministratore di sistema, ovvero il soggetto cui sono affidati i privilegi di Amministratore del sistema informatico (persona fisica), è la figura professionale che sovraintende alla gestione ed alla manutenzione di sistemi di elaborazione di cui è dotata l'Amministrazione, con particolare riferimento alla configurazione degli stessi, nonché alla gestione e alla manutenzione delle banche dati. Nell'ambito dell'organizzazione è possibile individuare tipologie specifiche di amministratore di sistema, differenziate per livello di autorizzazione e profilo.
2. L'attribuzione delle funzioni di gestore dei privilegi di amministratore del sistema informatico avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto della normativa in vigore sul trattamento dei dati e sulla sicurezza informatica. La designazione dell'Amministratore di sistema

è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

3. L'Amministratore di sistema svolge attività, quali, a titolo esemplificativo e non esaustivo:
    a) pianificare, eseguire e verificare l'organizzazione dei flussi di rete, la corretta esecuzione del backup e delle copie, la gestione dei supporti di memorizzazione e la manutenzione hardware;
    b) proporre l'introduzione ed integrazione di nuove tecnologie negli ambienti esistenti;
    c) installare e configurare nuovo hardware/software sia lato client che lato server;
    d) applicare le patch e gli aggiornamenti necessari al software di base applicativo, modificare la configurazione in base all'esigenze della Amministrazione;
    e) gestire e mantenere aggiornati gli account utente relativi ai profili di autorizzazione;
    f) fornire risposte a questioni tecniche di competenza sollevate dagli utenti;
    g) affrontare ed attivarsi per risolvere problemi, guasti o malfunzionamenti.
4. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'Amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.
5. Secondo la normativa vigente, l'operato dell'Amministratore di sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.
6. Il Titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
7. L'Amministratore di sistema è destinatario degli interventi di formazione e di aggiornamento.

Art. 30 - Coordinamento con Amministrazione trasparente, procedimenti di accesso civico, generalizzato e documentale

1. Costituisce onere sia del RPD che del Responsabile per la prevenzione della corruzione e della trasparenza coordinare le loro attività al fine di semplificare e minimizzare l'impatto degli adempimenti sull'attività degli uffici/servizi e garantire la massima protezione dei dati personali ogni

qualvolta procedimenti di ufficio o attivati su istanza di soggetti esterni comportino attività di pubblicazione dei dati personali in Amministrazione trasparente, il rilascio di dati personali in occasione di istanze di accesso civico, generalizzato e documentale. In tali ultime ipotesi dovranno essere adottate misure di sicurezza adeguate compresa la minimizzazione dei dati personali.

2. Negli atti destinati alla pubblicazione o divulgazione, i dati che permettono di identificare gli interessati sono riportati quando è necessario ed è previsto da una norma di legge mentre in tutti gli altri casi ciò deve avvenire rispettando il principio di proporzionalità, mediante la verifica che tale pubblicazione a fini di trasparenza concerne solo dati pertinenti e non eccedenti rispetto alle finalità perseguite.

Art. 31 - Attività amministrativa

1. L'attività amministrativa dell'Ente si svolge, principalmente, con la emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.
2. Tutta l'attività di gestione dei dati deve essere pertanto ispirata a:
    a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati;
    b) prevenire:
        - trattamenti dei dati non conformi alla legge o ai regolamenti;
        - cessione o distribuzione dei dati in caso di cessazione del trattamento.
3. Per l'attività informatica di cui al comma 1 sono rispettate le norme di cui al codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni ed integrazioni.
4. La sicurezza dei dati personali è assicurata anche mediante adeguate soluzioni tecniche connesse all'utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche.

Art. 32 - Sicurezza del trattamento

1. Il livello di sicurezza da assicurare nel trattamento dei dati è valutato tenuto conto dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
2. L'Ente, ciascun Designato e ciascun Responsabile del trattamento, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, mettono in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e

delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

3. Le misure tecniche ed organizzative di sicurezza utilizzabili da parte dei soggetti di cui al comma precedente per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
4. Costituiscono inoltre misure tecniche ed organizzative che possono essere adottate dal servizio cui è preposto ciascun Designato (responsabile interno) del trattamento:
   - sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
   - sistemi di rilevazione di intrusione; sistemi di sorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
5. Il Titolare e ciascun Responsabile del trattamento sono tenuti ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. Restano in vigore le misure di sicurezza attualmente previste, le limitazioni alla diffuzione e alla pubblicazione per i trattamenti di particolari tiologie di dati, c.d. dati sensibili, per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi.

Art. 33 - Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto dell'Ente , del Titolare, eventualmente del Contitolare del trattamento, e del RPD;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 32.

2. Il Registro unico del trattamento è tenuto dal Titolare, presso la sede dell'Ente in forma telematica/cartacea; nello stesso possono essere inserite ulteriori informazioni tenuto conto di specifiche necessità organizzative e funzionali dell'Ente stesso.
3. Nel caso di cui al precedente comma, il Titolare può, sotto la propria responsabilità, decidere di affidare la tenuta di tale registro unico al RPD. Ciascun Designato ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico. Resta, invece, fermo l'obbligo per i Responsabili esterni del trattamento di tenere distintamente il registro delle attività di trattamento ed il registro delle categorie di attività trattate.

Art. 34 - Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Designato del trattamento reca le seguenti informazioni:
   i. il nome ed i dati di contatto del Designato del RPD;
   ii. le categorie di trattamenti effettuati da ciascun Designato o Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
   iii. l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   iv. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 32.

Art. 35 - Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, in particolare allorché questo prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 del RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, del RGDP.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, del

RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

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

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che esso non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa.
Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Ente .
Il Titolare può consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni

assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

5. Il Designato del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
6. L'ufficio competente per la sicurezza dei sistemi informativi fornisce supporto al Titolare per lo svolgimento della DPIA.
7. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
8. La DPIA non è necessaria nei casi seguenti:
    i. se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, del RGDP;
    ii. se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
    iii. se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
    iv. se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
9. Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.
10. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
    a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
    b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
        - delle finalità specifiche, esplicite e legittime;
        - della liceità del trattamento;
        - dei dati adeguati, pertinenti e limitati a quanto necessario;

- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

11. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
12. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
13. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 36- Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Titolare.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore

dal primo accertamento del verificarsi dell'evento e comunque senza ingiustificato ritardo.

3. Il Responsabile esterno del trattamento notifica al Titolare ogni violazione di dati a carattere personale nel tempo massimo di 24 ore, a mezzo pec. I Designati sono obbligati ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione.
4. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
    A. danni fisici, materiali o immateriali alle persone fisiche;
    B. perdita del controllo dei dati personali;
    C. limitazione dei diritti, discriminazione;
    D. furto o usurpazione d'identità;
    E. perdite finanziarie, danno economico o sociale.
    F. decifratura non autorizzata della pseudonimizzazione;
    G. pregiudizio alla reputazione;
    H. perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
5. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
    a. coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
    b. riguardare categorie particolari di dati personali
    c. comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze)
    d. comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
    e. impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
6. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
7. Il Titolare deve opportunamente documentare, mediante la istituzione di un registro, le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art. 37 – Pubblicazione sintesi della valutazione d'impatto – DPIA

1. Il Titolare effettua la pubblicazione della DPIA o di una sintesi della stessa al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal Titolare, nonché di dimostrare la responsabilizzazione e la trasparenza.
2. La DPIA pubblicata non deve contenere l'intera valutazione qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il Titolare o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

Art. 38 – Consultazione preventiva

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

Art. 39 – Modulistica e procedure

1. Il Titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del RGPD, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante
   a) adotta e costantemente aggiorna:
      - modelli uniformi di informativa;
      - modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;
   b) elabora, approva, e costantemente aggiorna adeguate procedure gestionali.

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

1. Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è sanzionato con le sanzioni previste da parte del Garante, nonché con sanzioni di natura disciplinare.
2. Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.
3. Il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi previsti nel Codice, nel RGPD e nel presente regolamento, e a lui specificamente diretti o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal Titolare del trattamento.
4. Il Titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 41 – Principio di collaborazione

1. Tutto il personale coinvolto nelle procedure di trattamento dati, a qualunque livello e ruolo:
    i. collabora con il Titolare, il RPD, l'Autorità di controllo ed eventuali ulteriori soggetti addetti alla vigilanza, controllo ed attuazione delle disposizioni in materia di trattamento dei dati fornendo la massima e tempestiva collaborazione con particolare riferimento al rispetto dei principi previsti dal RGPD;
    ii. fornisce tempestivamente informazioni su potenziali pericoli, rischi, o violazioni dei dati personali anche al fine di consentire l'esercizio dei compiti di cui all'art. 33 e 34 del RGPD (cosiddetto "data breach");
    iii. collabora con i Designati del trattamento, secondo le istruzioni fornite dal Titolare, al fine di garantire le citate finalità e nel rispetto degli obblighi di segretezza e riservatezza.
    iv. si impegna a rispettare le previsioni normative di livello europeo, nazionale e regolamentare per la tutela dei dati personali.
2. Il rispetto dei principi in materia e dei compiti e adempimenti previsti dal presente provvedimento verrà valutato in sede di raggiungimento degli obiettivi e/o negli altri casi di responsabilità del personale a vario titolo coinvolto.

Art. 42 – Disposizioni finali

1. Per quanto non previsto nel presente Regolamento, si rinvia al “Regolamento generale sulla protezione dei dati (UE)2016/679”, alle vigenti fonti di diritto europee e nazionali, con particolare riferimento al dlgs 196/2003 e ai regolamenti comunali in materia di protezione dei dati personali, alle linee guida e ai provvedimenti del “Gruppo di Lavoro 29” nonché del Garante della Privacy, alle direttive impartite dal Titolare del trattamento e dai Responsabili del trattamento, dall’Amministratore del sistema informatico e dal Responsabile della protezione dei dati.