Città di Pescia

REGOLAMENTO COMUNALE SULLA PROTEZIONE DEI DATI PERSONALI ADOTTATO IN ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679

(approvato con delibera C.C. n. ... del ../../2021)

SOMMARIO

CAPO I - DISPOSIZIONI GENERALI

Art. 1: Oggetto

Il presente Regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal titolare, nel rispetto di quanto previsto dal GDPR.

Art. 2: Definizioni

Il presente regolamento si avvale delle seguenti definizioni:

a. "**Codice**": D.Lgs. n. 196/2003, come modificato dal D.Lgs. 101/2018;
b. "**GDPR**": il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
c. "**Regolamento sui dati sensibili**": il Regolamento interno, approvato dal Titolare in conformità allo schema tipo approvato dal Garante, che identifica e rende pubblici, per i trattamenti dei dati sensibili e giudiziari, i tipi di dati e le operazioni eseguibili;
d. "**Regolamento**": il presente Regolamento
e. "**Titolare**": il Comune di Pescia
f. **"Dirigenti/Responsabili di P.O."**: i soggetti che esercitano i poteri delegati dal titolare o che sono nominati dal titolare per esercitare tali poteri.

Il presente regolamento recepisce le definizioni del D.Lgs. n. 196/2003 e del GDPR, fermo restando che, in caso di discordanza, prevalgono le definizioni contenute nei suddetti testi normativi:

A) Definizioni ai sensi del D.Lgs. n. 196/2003 (in ordine alfabetico)**:**

- "**Autenticazione informatica**": l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- "**Banca di dati**": qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- "**Blocco**": la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- "**Chiamata**": la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;
- "**Comunicazione**": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "**Comunicazione elettronica**": ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;
- "**Contraente**": qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario ditali servizi tramite schede prepagate;
- "**Credenziali di autenticazione**": i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- "**Dati giudiziari**": i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "**Dati identificativi**": i dati personali che permettono l'identificazione diretta dell'interessato;
- "**Dati relativi al traffico**": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- **"Dati relativi all'ubicazione**": ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

- "**Dati sensibili**": i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "**Dato anonimo**": il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- "**Dato personale**": qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "**Diffusione**": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "**Garante**": l'autorità di cui all'articolo 153 D.Lgs. 196/2003;
- "**Incaricati**": le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- "**Interessato**": la persona fisica, cui si riferiscono i dati personali;
- "**Misure minime**": il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31D.Lgs.n. 196/2003;
- **"Parola chiave**": componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati informa elettronica;
- **"Posta elettronica**": messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;
- "**Profilo di autorizzazione**": l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- "**Responsabile**": la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal al trattamento di dati personali;
- "**Reti di comunicazione elettronica**": i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- "**Rete pubblica di comunicazioni**": una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni trai punti terminali di reti;
- "**Scopi scientifici**": le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore;
- "**Scopi statistici**":le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- "**Scopi storici**": le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- "**Servizio a valore aggiunto**": il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto e' necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- "**Servizio di comunicazione elettronica**": i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- "**Sistema di autorizzazione**": l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
- "**Strumenti elettronici**": gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

- "**Titolare**": la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "**Trattamento**": qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "**Trattamenti effettuati per finalità amministrativo–contabili**": i trattamenti connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute,igiene e sicurezza sul lavoro
- "**Utente**": qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- "**Violazione di dati personali**": violazione della sicurezza che comporta, anche accidentalmente, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico;

B) definizioni ai fini del GDPR (in ordine alfabetico)**:**

- "**Archivio**": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- "**Autorità di controllo**": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;
- "**Autorità di controllo interessata**": un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    - il Titolare del trattamento o il Responsabile del trattamento è stabilito sul–territorio dello Stato membro di tale autorità di controllo;
    - gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
- "**Consenso dell'interessato**": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- "**Dati biometrici**": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- "**Dati genetici**": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- "**Dati relativi alla salute**": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- "**Dato personale**": qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- "**Destinatario**": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il

trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- "**Gruppo imprenditoriale**": un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- "**Impresa**": la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- "**Limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- "**Norme vincolanti d'impresa**": le politiche in materia di protezione dei dati personali applicate da un Titolare del trattamento o Responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un Titolare del trattamento o Responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- "**Obiezione pertinente e motivata**": un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del GDPR, oppure che l'azione prevista in relazione al Titolare del trattamento o Responsabile del trattamento sia conforme al GDPR, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
- "**Organizzazione internazionale**": un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati;
- "**Profilazione**": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **"Pseudonimizzazione**": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- "**Rappresentante**": la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- "**Responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- "**Servizio della società dell'informazione**": il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- "**Stabilimento principale**": per quanto riguarda un Titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua Amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; con riferimento a un Responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua Amministrazione centrale nell'Unione o, se il Responsabile del trattamento non ha un'Amministrazione centrale nell'Unione, lo stabilimento del Responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del Responsabile del trattamento nella misura in cui tale Responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
- "**Terzo**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- "**Titolare del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o

degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- "**Trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma dimessa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- "**Trattamento transfrontaliero**": trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del trattamento o Responsabile del trattamento nell'Unione ove il Titolare del trattamento o il Responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare del trattamento o Responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- "**Violazione dei dati personali**": la violazione di sicurezza che comporta, accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Ai fini meramente esemplificativi, si riporta (ALL. A) il grafico riepilogativo delle principali definizioni ed istituti fondamentali.

Art. 3: Quadro normativo di riferimento

Il presente Regolamento tiene conto dei seguenti documenti:

- Codice in materia di dati personali (D.Lgs. n.196/2003, come modificato dal D.Lgs. 101/2018);
- Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. n.196/2003);
- Linee guida e raccomandazioni del Garante;
- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- Legge 25 ottobre 2017, n. 163 (art. 13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;
- D.Lgs. n. 10 agosto 2018, n. 101, di adeguamento della normativa interna al GDPR *(Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati.*

ART. 4: Finalità del trattamento

1. I trattamenti sono compiuti dal Comune 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:
        i. 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;
        ii. la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
        iii. l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

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

CAPO II – PRINCIPI

Art. 5: Principi e responsabilizzazione

Vengono integralmente recepiti, nell'ordinamento interno del titolare, i principi del GDPR, per effetto dei quali 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 considerato incompatibile con le finalità iniziali;
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati base del 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 base del principio di "esattezza";
e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "limitazione della conservazione";
f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali 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*").

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 GDPR in ordine alla liceità del trattamento e, dunque, 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) non si applica al trattamento di dati effettuato dal titolare nell'esecuzione dei propri compiti e funzioni.

Art. 7: Condizioni per il consenso

1. Fermi restando i casi nei quali può essere legittimamente effettuato il trattamento senza consenso in quanto 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 Comune (art. 6, co. 1, lette. e, del GDPR) e per gli altri casi dello stesso art. 6, co. 1, nei casi in cui il trattamento dei dati personali, per una o più specifiche finalità, è subordinato al consenso dell'interessato, si applica la disciplina del GDPR (art. 7), la quale prevede che:
    a. qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
    b. se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante;
    c. l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato;
    d. nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.
    e. per i dati sensibili il consenso deve essere esplicito e in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;
    f. il consenso dei minori è valido a partire dai 16 anni (art. 8, co. 1, del GDPR), fermo restando il diverso limite di età, comunque non inferiore a 13 anni, previsto dalla normativa nazionale; prima del limite di età previsto dalla normativa nazionale occorre raccogliere il consenso dei genitori o di chi ne fa le veci;
    g. deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle prespuntate su un modulo);
    h. deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".
2. In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.

Art. 8: 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 dagli articoli 13 e 14 del GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
2. L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.
3. L'informativa è fornita, mediante idonei strumenti:
    a. attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti;
    b. avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture comunali e in altri locali in cui ha accesso l'utenza;
    c. apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il titolare;

d. resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alle procedure.

4. L'informativa contiene il contenuto minimo previsto dall'art. 13 del GDPR 679/2016.
5. Nel caso di dati personali non raccolti direttamente presso l'interessato si applica l'art. 14 del GDPR 679/2016.
6. Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del titolare è predisposta apposita informativa per personale dipendente.
7. Apposite informative devono essere inserite nei seguenti documenti:
    a. nei bandi e nella documentazione di affidamento dei contratti pubblici, nei contratti, accordi o convenzioni, nei bandi di concorso pubblico, nelle segnalazioni di disservizio e, più in generale, in ogni altro documento contenente dati personali.
8. Nel fornire l'informativa, il titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

Art. 9: Sensibilizzazione e formazione

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.

CAPO III - IL TRATTAMENTO DEI DATI PERSONALI

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

1. Il titolare tratta i dati personali per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Codice, dal GDPR e dalle Linee guida e dai provvedimenti del Garante.
2. Il titolare effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:
    a. la gestione del personale dipendente, ivi comprese le procedure di assunzione;
    b. la gestione dei soggetti che intrattengono rapporti giuridici con il titolare, diversi dal rapporto di lavoro dipendente, e che operano a qualsiasi titolo all'interno della struttura organizzativa del titolare, ivi compresi gli stagisti, tirocinanti e i volontari;
    c. la gestione dei rapporti con i consulenti, i libero-professionisti, i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione lavori, opere e di interventi di manutenzione;
    d. la gestione dei rapporti con i soggetti accreditati o convenzionati per i servizi socio-assistenziali;
    e. la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti;

f. la gestione dei rapporti derivanti da ordinanze contingibili ed urgenti del Sindaco, nonché dalle ordinanze emanata dai Dirigenti competenti.

3. Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del titolare, solo da parte dei soggetti appositamente autorizzati:
   a. Titolare
   b. Dirigenti, in qualità di soggetti che esercitano i poteri delegati dal titolare o in qualità di soggetti nominati dal titolare per l'esercizio di tali poteri
   c. Dipendenti, in qualità di incaricati del trattamento.
4. Non è consentito il trattamento da parte di persone non autorizzate.
5. Ai fini del trattamento, il titolare provvede, in collaborazione con i dirigenti, alla integrale ricognizione e all'aggiornamento di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti del titolare medesimo, funzionali alla formazione dell'indice dei trattamenti.
6. E' compito dei dirigenti effettuare e documentare l'aggiornamento periodico, almeno annuale, della ricognizione dei trattamenti e del relativo indice, e la valutazione periodica, infrannuale, del rispetto dei principi di cui all'art. 5 del presente Regolamento con riferimento a tutti trattamenti inclusi nell'indice.
7. Il titolare, i dirigenti e gli incaricati si attengono alle modalità di trattamento indicate nel Codice, nel GDPR, nonché nelle disposizioni attuative e nelle Linee guida del Garante per la protezione dei dati personali.

Art. 11: Tipologie di dati trattati

1. Nell'ambito dei trattamenti inclusi nell'indice dei trattamenti, il titolare, nell'esercizio delle sue funzioni istituzionali, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:
   a. Dati comuni identificativi
   b. Dati sensibili
   c. Dati giudiziari

Art. 12: Trattamento 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 di cui ai Consideranda n. da 51 a 57 ed agli articoli 9 e 10 del GDPR per il trattamento di dati sensibili e giudiziari, nonché le pertinenti disposizioni del GDPR, e si conforma alle Linee Guida del Garante in materia (*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, 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, dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1*).
3. Il titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati sensibili e giudiziari.
4. In fase di prima applicazione, ai fini dell'identificazione dei dati sensibili e giudiziari per i quali è consentito il relativo trattamento, nonché le operazioni eseguibili in relazione alle specifiche finalità di interesse pubblico perseguite, si fa riferimento alle tabelle allegate alla delibera C.C. n. 104 del 21.12.2005).
5. Entro il termine di 12 mesi dall'approvazione del presente Regolamento, i Dirigenti provvederanno ad apportare gli aggiornamenti, le integrazioni e le modifiche che si rendono necessarie a causa di normative sopravvente e il Dirigente Affari Generali porterà le tabelle nuove in Consiglio Comunale per la loro approvazione.

Art. 13: 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 od 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, nel trattamento dei dati sensibili relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.
8. 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. 14: Registro delle attività di trattamento e delle categorie di trattamento

1. Ai sensi dell'art. 30, co. 1, del GDPR, il titolare del trattamento istituisce un registro, in forma scritta, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità.
2. Il registro deve contenere tutte le informazioni indicate nello stesso art. 30, co. 1, del GDPR e deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo.
3. Ai sensi dell'art. 30, co. 2, del GDPR, il responsabile di trattamento tiene registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento.
4. I registri sono tenuti in forma scritta, anche in formato elettronico.
5. Il registro deve contenere tutte le informazioni indicate nello stesso art. 30, co. 2, del GDPR e deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo.
6. Su richiesta, il titolare del trattamento o il responsabile del trattamento, mettono il registro a disposizione del Garante.

CAPO IV – DIRITTI DEGLI INTERESSATI

Art. 15: Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. Il Titolare, in sede di pubblicazione e diffusione, tramite l'albo pretorio informatico e la rete civica, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:
    a. Sicurezza
    b. Completezza
    c. Esattezza
    d. Accessibilità

    e. Legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.
2. Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, tranne deroghe previste da specifiche disposizioni e in coordinamento con le disposizioni sulla trasparenza di cui al D.Lgs. 33/2013 e/o ad altre disposizioni normative.
3. Salva diversa disposizione di legge, il titolare garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on line o sulla rete civica, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.
4. In ogni caso, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere sensibile o giudiziario dell'interessato, devono essere anonimizzati con adeguate tecniche di anonimizzazione.
5. I dati sensibili e giudiziari sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.
6. Il titolare si conforma alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.

Art. 16: 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. 17: 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, di seguito elencati, in conformità alla disciplina contenuta nel Capo III (articoli da 12 a 22) del GDPR e nel Codice (con particolare riferimento agli articoli 2-undecies, 2-duodecies e 2-terdecies).

Art. 18: Diritto di accesso

1. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di accesso (art. 13 e ss. del GDPR) secondo la quale l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
    a. le finalità del trattamento;
    b. le categorie di dati personali in questione;
    c. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
    d. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
    e. l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
    f. il diritto di proporre reclamo a un'autorità di controllo;
    g. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

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

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.
4. 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.
5. Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Art. 19: Diritto alla rettifica e cancellazione

1. Ai sensi degli articoli 16, 17 e 19 del GDPR, il presente Regolamento tiene conto della disciplina del GDPR 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 GDPR;
    d. a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
    e. per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 20: Diritto alla limitazione

1. Il presente Regolamento tiene conto della disciplina del GDPR (artt. 18 e 19) 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 GDPR, 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 GDPR, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
4. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 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. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 21: Diritto alla portabilità

1. Il diritto alla portabilità dei dati è regolato dall'art. 20 del GDPR e consiste nel diritto dell'interessato di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento e il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti. Esso si applica qualora ricorrano i casi previsti dal paragrafo 1 dell'art. 20 del GDPR.
2. Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 20, paragrafo 3, del GDPR).

Art. 22: Diritto di opposizione

1. Il diritto di opposizione è regolato dall'art. 21 del GDPR e consiste nel diritto dell'interessato 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.
2. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il diritto di cui ai paragrafi 1 e 2 dell'art. 21 GDPR è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
3. Per tutto quanto non disciplinato dal presente articolo, si applica l'art. 21 del GDPR.

Art. 23: Processo decisionale automatizzato relativo alle persone

1. Il processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione è disciplinato dall'art. 22 del GDPR. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Per tutto quanto non disciplinato dal presente articolo, si applica l'art. 22 del GDPR.

Art. 24: Diritto di proporre reclami e ricorsi

1. Il titolare dei dati ha il diritto di rivolgersi alle Autorità amministrative e giurisdizionali in sede penale, civile ed amministrativa secondo quanto previsto dall'ordinamento giuridico italiano ed europeo e previsto dalla vigente legislazione.
2. Oltre a quanto sopra, l'interessato ha diritto, altresì a:
    a. Diritto di proporre reclamo all'autorità di controllo ai sensi dell'art. 77 del GDPR;
    b. Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo ai sensi dell'art. 78 del GDPR;

c. Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento ai sensi dell'art. 79 del GDPR;
d. Diritto al risarcimento ai sensi dell'art. 82 del GDPR;
e. Il diritto di opposizione è regolato dall'art. 21 del GDPR e consiste nel diritto dell'interessato 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.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 25: Modalità di esercizio dei diritti dell'interessato

1. Nel rispetto dei principi di cui all'art. 12 del GDPR, per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR medesimo, 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. L'interessato può presentare o inviare la richiesta di esercizio dei diritti:
    a. al titolare o Responsabile del trattamento, che conserva e gestisce i dati personali dell'interessato;
    b. all'ufficio protocollo generale del Comune o all'ufficio per le relazioni con il pubblico.
    c. 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. Fermo restando l'accesso ai dati personali, il dirigente autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.
5. I soggetti competenti alla valutazione dell'istanza sono il dirigente competente per materia o un suo delegato, 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. 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.
7. L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.
8. Il titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.
9. Per tutto quanto non disciplinato dal presente articolo, si applica l'art. 12 del GDPR.

Art. 26: Indagini difensive

1. Ai fini delle indagini svolte nel corso di un procedimento penale, per la richiesta di documenti da parte del difensore si applicano la Legge 7 dicembre 2000, n. 397 ("*Disposizioni in materia di indagini difensive* ") e l'art. 391-quater del Codice di procedura penale.
2. Il titolare e/o il responsabile si conformano alle Linee guida del Garante in tema di indagini difensive.

CAPO V – SOGGETTI

Art. 27: Titolare e contitolari

1. Ai sensi degli artt. 24 e ss. del GDPR, il titolare del trattamento è il Comune di Pescia, rappresentato dal Sindaco pro tempore, in qualità di legale rappresentante del titolare.
2. Il titolare provvede:
    a. a definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento, provvedendo all'inserimento di tali obiettivi strategici nel DUP e negli altri documenti di programmazione e pianificazione del titolare;
    b. a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Codice, al GDPR e al presente Regolamento;
    c. a delegare ovvero a nominare, con proprio atto, i dirigenti per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti, e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi, le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
    d. a formare e aggiornare l'elenco dei dirigenti delegati o nominati, e a pubblicarlo sul sito web istituzionale del titolare;
    e. a designare, con proprio atto, il Responsabile per la protezione dei dati personali;
    f. a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
    g. a favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
    h. a favorire l'adesione a meccanismi di certificazione;
    i. ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa;
3. Qualora il titolare si trovi in rapporto di contitolarità con altri titolari (cioè quando determinano congiuntamente le finalità e i mezzi del trattamento) si applica l'art. 26 del GDPR.

Art. 28: Dirigenti e Responsabili di Posizione Organizzativa – P.O.

1. Il titolare conferisce i sotto indicati compiti e funzioni, e i correlati poteri, mediante apposito provvedimento di delega o di nomina, ai dirigenti/P.O., in qualità di Responsabile del trattamento ai sensi dell'art. 28 del GDPR.
2. Nel suddetto provvedimento, il titolare deve informare ciascun dirigente, delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento.
3. Compiti, funzioni e poteri:
    a. trattare i dati personali su istruzione del titolare del trattamento;
    b. garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
    c. adottare il tempestivo ed integrale rispetto dei doveri del titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del GDPR;
    d. osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal titolare;

e. adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;
f. collaborare con il titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in collaborazione con l'amministratore di sistema e con le altre strutture competenti del titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
g. curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del titolare per l'applicazione del Codice, del GDPR, e del presente Regolamento;
h. assistere il titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
i. assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;
j. mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, GDPR e nel presente Regolamento;
k. contribuire alle attività di verifica del rispetto del Codice, del GDPR e del presente regolamento, comprese le ispezioni, realizzate dal titolare o da un altro soggetto da questi incaricato;
l. curare la costituzione e l'aggiornamento dei seguenti archivi/banche dati, per quanto di competenza:
    i. elenco dei contitolari, dei responsabili dei trattamenti, e degli incaricati, con i relativi punti di contatto;
    ii. elenco degli archivi/ banche;
m. garantire l'aggiornamento, almeno annuale, della ricognizione dei trattamenti;
n. fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni;
o. predisporre le informative previste e verificarne il rispetto e fornire le informazioni necessarie per l'aggiornamento del registro dei trattamenti;
p. designare gli incaricati del trattamento, e fornire loro specifiche istruzioni;
q. 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;
r. garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della struttura organizzativa del titolare ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali responsabili del trattamento;
s. informare il titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

4. Ciascun dirigente risponde al titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.
5. I dirigenti sono destinatari degli interventi di formazione di aggiornamento.

Art. 29: Responsabili del trattamento e sub responsabili

1. Il Responsabile ai sensi dell'art. 28 del GDPR è il soggetto che agisce per conto del titolare.
2. Il Responsabile è designato dal titolare. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In particolare, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
4. Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del titolare.
5. Il titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali, può designare quali Responsabili del trattamento dei dati personali, unicamente i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato (GDPR, art. 28).
6. I Responsabili del trattamento hanno l'obbligo di:
    a. trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia;
    b. 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;
    c. nominare al loro interno i soggetti incaricati del trattamento;
    d. garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento;
    e. attenersi alle disposizioni impartite dal Titolare del trattamento;
    f. specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti;
    g. comunicare le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
7. Nel caso di mancato rispetto delle predette disposizioni, e in caso di mancata comunicazione al titolare dell'atto di nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso il titolare, il Responsabile del trattamento.
8. La designazione del Responsabile viene effettuata mediante atto da parte del titolare del trattamento da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente al titolare.
9. L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Art. 30: Incaricati del trattamento dipendenti del titolare

1. Gli incaricati del trattamento sono le persone fisiche, dipendenti del titolare, designati da ciascun dirigente, incaricati di svolgere le operazioni di trattamento dei dati personali di competenza con l'indicazione specifica dei compiti, dell'ambito di trattamento consentito, e delle modalità.
2. La designazione dell'incaricato al trattamento dei dati personali è di competenza del dirigente; la nomina è effettuata per iscritto e individua specificatamente i compiti spettanti all'incaricato e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.
3. A prescindere dalla nomina, si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Per effetto di tale disposizione, ogni dipendente preposto ad un determinato ufficio/servizio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, è da considerare, "incaricato" ai sensi dell'art. 4 comma 10 del GDPR.
4. Gli incaricati devono comunque ricevere idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attività sui dati affidate e gli adempimenti a cui sono tenuti.

5. Gli incaricati collaborano con il titolare ed il dirigente segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.
6. In particolare, gli incaricati devono assicurare che, nel corso del trattamento, i dati siano:
    a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
    b. raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
    c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
    d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
    e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità pel quali i dati sono trattati;
    f. trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.
7. Gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propri attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal titolare e dal dirigente, nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del titolare.
8. Gli incaricati dipendenti del titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 31: Incaricati del 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 e i soggetti che operano temporaneamente all'interno della struttura organizzativa del titolare o incaricati nominati dal Responsabile esterno, devono essere incaricati del trattamento tramite atto scritto di nomina.
2. Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli incaricati dipendenti del titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
3. Gli incaricati non dipendenti dal titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 32: Amministratore di sistema

1. L'amministratore di sistema, individuato nel Responsabile del Centro Elaborazione Dati (CED) del Comune, sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.
2. La nomina dell'amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. 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 il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.
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.
5. Le registrazioni *(access log*) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
6. 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.

7. 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.
8. 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.
9. L'amministratore di sistema è destinatario degli interventi di formazione di aggiornamento.

Art. 33: Responsabile della protezione dei dati personali (RPD) - Data Protection Officer (DPO)

1. Ai sensi degli articoli 37 e ss. del GDPR, il Titolare designa il Responsabile della protezione dei dati (RPD/DPO).
2. Il RPD/PDO deve essere in possesso di:
    a. un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
    b. deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
    c. operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.
3. Il RPD/PDO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
4. Il titolare del trattamento mette a disposizione del RPD/DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.
5. Il RPD/PDO svolge i seguenti compiti:
    a. informa e fornisce consulenze al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
    b. verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
    c. fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
    d. funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
    e. funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

CAPO VI - SICUREZZA DEI DATI PERSONALI

Art. 34: Misure di sicurezza

1. Ai sensi dell'art. 32 del GDPR, il titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate e misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
2. In particolare il titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono almeno:
    a. la pseudonimizzazione e la cifratura dei dati personali trattati;
    b. procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
    c. modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
    d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Per quanto attiene al trattamento dei dati personali effettuato con strumenti elettronici e non, il titolare applica le misure minime ritenute adeguate in riferimento al proprio contesto.

ART. 35: Valutazione d'impatto sulla protezione dei dati – DPIA

1. Ai sensi degli artt. 35 e 36, la valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
2. La DPIA è uno strumento importante per la responsabilizzazione in quanto sostiene il titolare non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo GDPR.
3. I casi in cui deve essere adottata la DPIA, il procedimento di sua formazione, i casi in cui non è richiesta e il suo contenuto minimo sono disciplinati dagli articoli 35 e 36 del GDPR.
4. Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

Art. 36: 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. 37: 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 dagli articoli 166 (*), da 167 a 168 e da 170 a 172 del Codice, dagli articoli 83 e 84 del GDPR, 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 GDPR 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. l titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

(*) Gli articoli da 161 a 165, 169 del Codice 196/2003 sono stati abrogati dal D.Lgs. 101/2018

Art. 38: Notificazione di una violazione dei dati personali

1. In caso di violazione dei dati personali, si applica il procedimento previsto dall'art. 33 del GDPR.

Art. 39: Comunicazione di una violazione dei dati personali

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo, secondo le modalità di cui all'art. 34 del GDPR.

Art. 40: Disposizioni finali

1. Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, le Linee guida e i provvedimenti del Garante.
2. Il presente Regolamento si intende automaticamente aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.

ALL. A: GRAFICO RIEPILOGATIVO DELLE PRINCIPALI DEFINIZIONI ED ISTITUTI

SOGGETTI DELLA PRIVACY

DENOMINAZIONE	NORMATIVA D.Lgs. 196/2003	NORMATIVA Regolamento UE 679/2016 (GDPR)	NOTE	VARIE
Titolare del dato personale ("***interessato***")		Persona fisica identificata o identificabile alla quale è attribuibile il dato personale (art. 4)		
Titolare del trattamento		Persona fisica o giuridica (o autorità o organismo pubblici) che determina le finalità e i mezzi del trattamento (art. 4)	È una sorta di "regista" e protagonista principale della privacy	Ci possono essere più Titolari (contitolari) e i loro ambiti di competenza e responsabilità sono determinati da un accordo interno tra loro

RESPONSABILITA' E ADEMPIMENTI DEL TITOLARE:

1. Adottare tutte le misure adeguate per rispettare i principi del trattamento;
2. Adottare tutte le misure tecniche ed organizzative per garantire la protezione dei dati;
3. Nominare, per atto scritto, uno o più Responsabili del trattamento;
4. Designare il Responsabile della protezione;
5. Istruire il Responsabile;
6. Tenere un **REGISTRO DELLE ATTIVITA' DI TRATTAMENTO** (il cui contenuto è disciplinato dall'art. 30 del GDPR 679/2016); il Registro deve essere in forma scritta;
    a. Il Registro non deve essere tenuto dalle organizzazioni con meno di 250 dipendenti; ma anche in tali casi sussiste ugualmente l'obbligo qualora: a) il trattamento è rischioso per i diritti e le libertà dell'interessato; b) il trattamento non sia occasionale; c) il trattamento riguardi categorie di dati particolari (origine razziale, opinioni politiche, salute, orientamenti sessuali, aspetti penali, etc.). Per cui col presente Regolamento si ritiene che per i Comuni sia sempre obbligatorio, anche se hanno meno di 250 dipendenti
7. Notificare all'Autorità di controllo eventuali violazioni dei dati personali (entro 72 ore) (art. 33 del GDPR 679/2016)
    a. Se la violazione comporta un rischio elevato per i diritti dell'Interessato, deve comunicare anche a questi la violazione (tranne i casi di esenzione dalla comunicazione ex art. 34, co. 3, del GDPR 679/2016)
8. Effettuare una **VALUTAZIONE DELL'IMPATTO** prima di procedere al trattamento (e previa consultazione col Responsabile) quando un trattamento può presentare un elevato rischio per i diritti e le libertà delle persone fisiche (art. 35 del GDPR 679/2016)
    a. Il par. 3 dell'art. 35 indica i casi principali in cui vi è l'obbligo di valutazione dell'Impatto. In base al par. 4 l'Autorità di controllo

rende pubblico un elenco delle tipologie di trattamento per cui sussiste l'obbligo della valutazione dell'impatto

b. Il contenuto della Valutazione dell'impatto è disciplinato dal par. 7 dell'art. 35

c. Il Titolare deve, prima di iniziare un trattamento, consultare l'Autorità di controllo, qualora dalla valutazione dell'impatto risulti un grave rischio in assenza di misure idonee;

c.1. l'Autorità di controllo emette un parere scritto e può avvalersi dei poteri ex art. 58 (Poteri di indagine, correttivi – ingiunzioni, ammonimenti, avvertimenti, imposizione di limitazioni al trattamento, ordine di rettifica o cancellazione– , di accesso, di richiesta di informazioni, di applicazione della sanzione amministrativa pecuniaria

Responsabile del trattamento		art. 28 del GDPR 679/2016 Persona <u>fisica o giuridica</u> (o autorità o organismo pubblici) che tratta i dati personali per conto del titolare del trattamento. Può nominare un <u>sub-responsabile</u> (art. 28, par. 4) , ma deve essere autorizzato per iscritto dal Titolare. Il responsabile del trattamento risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile **,** anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" *(si veda art. 82, paragrafo 1 e paragrafo 3*	È il collaboratore principale del titolare.	

RESPONSABILITA' E ADEMPIMENTI DEL RESPONSABILE DEL TRATTAMENTO :

I rapporti tra Titolare e Responsabile sono regolati da "*<u>contratto o altro atto giuridico</u> ..... a norma del diritto..... che vincoli il Responsabile* " Occorre la <u>forma scritta</u>.

NOTA: Col presente Regolamento comunale, si ritiene che per le amministrazioni pubbliche possa bastare anche un atto autoritativo individuale, anche se l'art. 28 parla di "*stipulare*"; eventualmente il contratto (inteso come integrativo del contratto di lavoro principale) può essere utile per disciplinare il dettaglio (durata, strumenti, modalità concrete, eventuali compensi aggiuntivi, etc.). L'interpretazione contraria (cioè la necessarietà di un contratto, basato sul consenso delle due parti) rischierebbe di non poter avere un

Responsabile, qualora nessuno fosse disponibile). Egli deve:

1. Adottare tutte le misure tecniche e operative adeguate per rispettare i principi del trattamento;
2. Adottare tutte le misure tecniche ed organizzative per garantire la protezione dei dati;
3. Assistere il Titolare nel garantire l'esercizio dei diritti dell'Interessato e per garantire la sicurezza;
4. Fornire al Titolare tutte le informazioni che garantiscano il rispetto degli obblighi suddetti;
5. Informare il Titolare qualora ritenga che una sua istruzione sia illegittima;
6. Tenere un **REGISTRO DELLE ATTIVITA' DI TRATTAMENTO** (il cui contenuto è disciplinato dall'art. 30 del GDPR); il Registro deve essere in forma scritta;
   a. Il Registro non deve essere tenuto dalle organizzazioni con meno di 250 dipendenti; ma anche in tali casi sussiste ugualmente l'obbligo qualora: a) il trattamento è rischioso per i diritti e le libertà dell'interessato; b) il trattamento non sia occasionale; c) il trattamento riguardi categorie di dati particolari (origine razziale, opinioni politiche, salute, orientamenti sessuali, aspetti penali, etc.). Per cui, col presente Regolamento, si ritiene che per i Comuni è sempre obbligatorio, anche se hanno meno di 250 dipendenti
7. Informare il Titolare di eventuali violazioni dei dati personali (senza ritardo)
8. Adottare facoltativamente un Codice di condotta ex art. 40 e ss. del GDPR

Responsabile della protezione		Art. 37 e ss. del GDPR È possibile che più amministrazioni pubbliche designino insieme un unico Responsabile della protezione	Sono previsti vari casi in cui è obbligatorio designare il Responsabile della protezione. Per le P.A. l'obbligo è previsto dalla lettera a) del paragrafo 1 dell'art. 37: "*trattamento effettuato da un'autorità pubblica o da un organismo pubblico*".

RESPONSABILITA' E ADEMPIMENTI DEL RESPONSABILE DELLA PROTEZIONE: Egli deve:

1. Rispettare il segreto e la riservatezza;
2. Non ricevere istruzioni da altri per l'esecuzione dei suoi compiti;
3. Non svolgere altri compiti che possono comportare regime di conflitto di interessi;
4. Informare e fornire consulenza al Titolare e al Responsabile;
5. Sorvegliare l'osservanza del Regolamento UE circa le misure sulla protezione;
6. Fornire un parere per la Valutazione dell'impatto;
7. Cooperare con l'Autorità di controllo , per la quale funge da punto di contatto per tutte le questioni attinenti la sicurezza dei dati.

Incaricato del trattamento		Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 Codice, oggi abrogato dal D.Lgs. 101/2018), il regolamento non ne		

		esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" *(si veda, in particolare, art. 4, n. 10, del regolamento 679/2016).*		
Destinatario del dato personale		Persona fisica o giuridica (o autorità o organismo pubblici) che riceve comunicazione di dati personali		
Terzo		Persona fisica o giuridica (o autorità o organismo pubblici) che non sia uno dei soggetti di cui sopra		
Stabilimento principale		È il luogo ove il Titolare del trattamento ha la sua amministrazione principale nell'Unione	Stessa cosa vale per il Responsabile del trattamento	
Rappresentante		È chi rappresenta il Titolare o il Responsabile all'interno dell'Unione qualora costoro non siano stabiliti nell'Unione		
Impresa		Persona fisica o giuridica che esercita un'attività economica		
Gruppo imprenditoriale		Gruppo costituito da un'impresa controllante e da impresa/e controllata/e		

Autorità di controllo		Art. 51 e ss. del GDPR: È un'autorità pubblica e indipendente istituita in ciascuno Stato membro. All'interno di uno Stato possono esservi più Autorità di controllo	Sorveglia sull'applicazione del Regolamento	
Autorità di controllo interessata		È l'Autorità di controllo interessata perché Titolare, Responsabile o Interessato sono nel suo territorio nazionale.		
Compiti dell'autorità' di controllo		Sono elencati nell'art. 57 del GDPR; fra i più importanti: A) Sorvegliare sull'applicazione del Regolamento; B) **Trattare i reclami** proposti da un interessato; C) Svolgere indagini; D) Incoraggiare l'elaborazione di Codici di condotta; E) Effettuare un riesame periodico delle certificazioni ex art. 42, par. 7; F) Effettuare l'accreditamento di un organismo per il controllo dei Codici di condotta; G) Approvare le Norme vincolanti d'impresa; H) Svolgere **qualsiasi altro compito** legato alla protezione dei dati personali		
Poteri dell'Autorità di controllo		Sono elencati nell'art. 58 e sono classificati in 3 categorie: **Di indagine** – **Correttivi** – **Autorizzativi**. Fra i più importanti: A. **POTERI DI INDAGINE**: a. Ingiungere al Titolare di fornire informazioni; b. Accedere a tutti i dati personali , a tutte le informazioni e a tutti i locali del Titolare del trattamento; c. Effettuare un riesame delle certificazioni ex art. 42, par. 7 B. **POTERI CORRETTIVI**: a. Rivolgere **avvertimenti**, **ammonimenti** o **ingiunzioni** al Titolare o al Responsabile; b. Imporre limitazioni (provvisorie o definitive) o il divieto di trattamento; c. Ordinare la rettifica, la cancellazione di dati o la limitazione del trattamento; d. Infliggere una **sanzione amministrativa pecuniaria** ex art. 83		

		C. **POTERI AUTORIZATIVI**: a. Consulenza al Titolare del trattamento ex art. 36 ("Consultazione preventiva") b. Autorizza il trattamento nei casi di cui all'art. 36, par. 5 ("Consultazione preventiva") e se previsto dallo Stato membro c. Accredita organismi di certificazione Ogni Stato membro può conferirle, con legge, **ulteriori poteri**.
Comitato europeo per la protezione dei dati ("COMITATO")		Art. 68: è un organismo dell'Unione dotato di personalità giuridica e composto dalla figura di vertice di un'Autorità di controllo per ciascuno Stato membro e dal Garante Europeo per la protezione dei dati. Suo compito essenziale è garantire l'applicazione coerente del Regolamento in tutta l'Unione (art. 70). Emette parere ove un'Autorità di controllo debba adottare particolari misure (art. 64 e ss.) o quando viene richiesto da un?autorità di controllo, dal Presidente del Comitato stesso o dalla Commissione. Se l'Autorità di controllo non intende conformarsi al parere del Comitato, in alcuni casi specifici il Comitato emette una decisione vincolante. Contro le decisioni vincolanti del Comitato ciascuna Autorità di controllo di ciascuno Stato può avanzare impugnazione innanzi alla Corte di Giustizia (v. n. 143 del Consideranda); stessa cosa può fare qualsiasi persona fisica o giuridica.

TIPOLOGIA DI DATI

TIPOLOGIA	NORMATIVA D.Lgs. 196/2003	NORMATIVA Regolamento UE 679/2016 (GDPR)	NOTE	VARIE
Dato personale		Art. 4, n. 1 del GDPR. Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("*Interessato*")		
Dato sensibile		Art. 9 del GDPR 1) Origine razziale o etnica 2) Opinioni politiche 3) Convinzioni religiose o filosofiche	Per questi dati vi è il **divieto di trattamento**, a meno che non ricorrano le condizioni (**eccezioni**) di cui al paragrafo 2 dell'art.9	

		4) Appartenenza sindacale 5) Dati genetici 6) Dati biometrici 7) Salute, vita sessuale e orientamento sessuale		
Dato genetico		Art. 4, n. 13 GDPR Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite		
Dati biometrici		Art. 4, n. 14 GDPR Dati personali ottenuti da un trattamento tecnico specifico e relativi alle caratteristiche fisiche, fisiologiche o comportamentali e che consentono univoca di una persona	Esempio: una fotografia, dati dattiloscopici, etc.	
Dati relativi alla salute		Art. 4, n. 15 GDPR Dati personali relativi alla salute fisica e mentale		
Dati relativi a condanne penali, reati, misure di sicurezza		Art. 10 del GDPR Il trattamento può avvenire solo sotto il controllo dell'autorità pubblica		

PRINCIPI

Principio	**NORMATIVA D.Lgs. 196/2003**	**NORMATIVA Regolamento UE 679/2016 (GDPR)**	**NOTE**	**VARIE**
Liceità		I presupposti di legittimità del trattamento sono indicati nell'art. 6 del GDPR	Sono elencati vari casi riguardanti: a) l'esistenza di un consenso validamente espresso; b) vari casi di necessarietà del trattamento	
Correttezza		Art. 5, co. 1, lett. a),del GDPR Il Titolare deve fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR	I due articoli distinguono i casi di "dati raccolti presso l'interessato" e "dati non ottenuti presso l'interessato"	

Trasparenza		Art. 12 e ss. del GDPR L'obbligo di fornire all'interessato tutte le informazioni in modo conciso, trasparente, intelligibile e facilmente accessibile	a. Le informazioni richieste devono essere fornite "senza giustificato ritardo" e, comunque, entro 1 mese, prorogabile motivatamente a 2 mesi. b. Le informazioni sono gratuite c. Se non si ottempera, bisogna comunicare al richiedente i motivi dell'inottemperanza Per le richieste manifestamente infondate o eccessive e ripetitive (ma da dimostrare), il titolare o addebita un contributo spese o rifiuta di soddisfare la richiesta	
Limitazione delle finalità		Il trattamento può essere effettuato solo per finalità determinate, esplicite e legittime		
Adeguatezza, pertinenza e limitazione ("*minimizzazione dei dati*")		I dati trattati devono essere adeguati, pertinenti e necessari		
Esattezza e aggiornamento				
Limitazione della conservazione		I dati possono essere conservati per un arco di tempo non superiore al conseguimento delle finalità		
Sicurezza		Per i dati personali bisogna garantire un'adeguata sicurezza		
Responsabilizzazione		Il Titolare del trattamento è responsabile per i paragrafo 1 dell'art. 5 (liceità, correttezza e trasparenza) e deve poterlo comprovare		

DIRITTI DELL'INTERESSATO

TIPOLOGIA	NORMATIVA D.Lgs. 196/2003	NORMATIVA Regolamento UE 679/2016 (GDPR)	NOTE	VARIE
Diritto di accesso a tutte le informazioni sui dati che lo riguardano (art. 12, 13 e 14)		Art. 12/15 del GDPR		
Diritto a che gli vengano comunicate tutte le informazioni sui dati che lo riguardano (art. 12, 13 e 14)		Art. 12, 13 e 14 GDPR		
Diritto a revocare il consenso in qualsiasi momento		Art. 7, co. 2 GDPR		
Diritto alla rettifica dei dati		Art. 16 GDPR		
Diritto all'**OBLIO** (alla cancellazione dei dati)		Art. 17 GDPR	Il par. 3 indica i casi tassativi in cui il diritto alla cancellazione (all'oblio) non si applica	
Diritto di limitazione del trattamento		Art. 18 GDPR GDPR	In caso di trattamento limitato, i dati possono essere trattati solo col consenso dell'interessato, salvo le eccezioni previste dal par. 2	
Diritto alla portabilità dei dati		Art. 20 GDPR : è il diritto di trasmettere ad un altro Titolare del trattamento i propri dati personali detenuti da un Titolare del trattamento	L'interessato ha anche un diritto alla trasmissione diretta dei dati da un Titolare all'altro , se ciò e tecnicamente fattibili	
Diritto di opposizione		Art. 21 GDPR : è il diritto di opporsi al trattamento dei dati personali "necessari" e solo per 2 casistiche	Per i casi in cui il trattamento dei dati non è "necessario", è sottinteso e scontato che sussiste il diritto di opposizione	
Diritto a proporre **reclamo** all'Autorità di controllo		Art. 77 GDPR : il reclamo va presentato all'Autorità di controllo dello Stato in cui si risiede o si lavora o ove si è verificata la presunta violazione.		

		Il diritto di ricorso lascia salvo ogni altro ricorso amministrativo o giurisdizionale	
Diritto al **ricorso giurisdizionale** avverso l'Autorità di controllo		Art. 78 GDPR : il ricorso si può presentare per una decisione giuridicamente vincolante dell'Autorità oppure qualora essa non tratti un reclamo. Il ricorso si presenta innanzi all'autorità giurisdizionale dello Stato membro	
Diritto al **ricorso giurisdizionale** avverso il Titolare o il Responsabile del Trattamento		Art. 79 GDPR: il ricorso si presenta innanzi all'autorità giurisdizionale dello Stato membro ove il Titolare ha il suo stabilimento o in quello ove l'Interessato risiede abitualmente	
Diritto al **risarcimento**		Art. 82 GDPR : è risarcibile il danno sia materiale che immateriale causato dal Titolare o dal Responsabile , a meno che costoro non dimostrino che l'evento dannoso non è loro imputabile. L'azione legale si fa valere innanzi all'autorità giurisdizionale dello Stato membro	

ADEMPIMENTI DEGLI ENTI LOCALI

ADEMPIMENTO	**NORMATIVA D.Lgs. 196/2003**	**NORMATIVA Regolamento UE 679/2016 (GDPR)**	**NOTE**	**VARIE**
Tenuta del **registro delle attività di trattamento effettuate dal Titolare (Registro dei trattamenti)** *(art. 30, paragrafo 1 del GDPR)*;		Il contenuto di tale registro è elencato nel par. 1 dell'art. 30.	L'obbligo incombe sul Titolare del trattamento. Il registro deve essere in forma scritta, anche in formato elettronico	Non c'è l'obbligo per le organizzazioni con meno di 250 dipendenti, a meno che non vi siano rischi particolari per i diritti e le libertà dell'interessato oppure quando il trattamento non è occasionale. Praticamente per i Comuni è obbligatorio
Tenuta del **registro delle attività di trattamento effettuate dal Responsabile del trattamento (Registro dei trattamenti)** *(art. 30,*		Il contenuto di tale registro è elencato nel par. 2 dell'art. 30.	L'obbligo incombe sul Responsabile del trattamento . Il registro deve essere in forma scritta, anche in	IDEM

paragrafo 2 del GDPR);			formato elettronico	
Adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti *(art. 32, del GDPR)*;		Il contenuto di tale registro è elencato nell'art. 32.		
Art. 25 e 26: adozione, da parte del titolare, di **misure tecniche ed organizzative adeguate** per la **sicurezza** dei dati e per il rispetto del principio di **necessarietà** del trattamento (solo i dati personali necessari alla finalità)		Art. 25 del GDPR		
Art. 28: **Nomina del Responsabile del trattamento**, con atto scritto (contratto individuale e/o altro atto giuridico vincolante)		Art. 28: le caratteristiche ed i compiti sono indicati nell'art. 28, par. 3	L'incarico deve essere conferito per iscritto (contratto o altro atto giuridico vincolante)	
Art. 29: **istruzione** del Responsabile del procedimento		Art. 29 del GDPR		
Art. 37: **Nomina del Responsabile della protezione** dei dati, con atto scritto (contratto individuale e/o altro atto giuridico vincolante)		Art. 37 GDPR: le caratteristiche ed i compiti sono indicati negli art. 38 e 39	L'incarico deve essere conferito per iscritto (contratto o altro atto giuridico vincolante)	L'incarico può essere conferito ad un dipendente o ad un soggetto esterno (con contratto di servizi)

SANZIONI

VIOLAZIONE	**NORMATIVA D.Lgs. 196/2003**	**NORMATIVA Regolamento UE 679/2016 (art. 83, co. 4, 5 e 6**	**SOGGETTO**	**SANZIONE**	**NOTE**
ART. 8 GDPR: Non acquisizione del consenso dei		Art. 83, co. 4 e art. 8, co. 1 e 2 GDPR	Titolare o Responsabile del	Sanzione amministrativa pecuniarie **fino**	Gli stai membri possono stabilire un'età

minori di 16 anni nei casi di offerta diretta di servizi della società dell'informazione ai minori			trattamento	**a 10.000.000 EUR,** o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	inferiore, purché non inferiore a 13 anni
ART. 11 GDPR: Quando il titolare del trattamento non è in grado di dimostrare di non essere in grado di identificare l'interessato e, quindi, di non poter adempiere agli articoli da 15 a 22		Art. 83 GDPR, co. 4 e art. 11	Titolare del trattamento	IDEM	Gli articoli da 15 a 22 sono quelli che prevedono vari diritti dell'interessato: di accesso, di rettifica, di cancellazione (diritto all'oblio) diritto alla portabilità dei dati, etc.
ART. da 25 a 39 GDPR: Art. 25: Adozione mísure **tecniche ed organizzative adeguate** per la **sicurezza** dei dati e per il rispetto della **necessarietà** rispetto alla finalità (trattamento dei soli dati necessari)		Art. 83, co. 4 e art. 25 GDPR	Titolare del trattamento	IDEM	
ART. da 25 a 39 GDPR: Art. 27: Designazione, per iscritto, di un rappresentante nell'Unione		Art. 83, co. 4 e art. 27 GDPR	Titolare e Responsabile del trattamento	IDEM	Tale obbligo di designazione si applica solo nel caso di titolare di responsabile che non è stabilito nell'Unione

ART. da 25 a 39 GDPR: Art. 28: Nomina del **Resposnsabile del trattamento**, con atto scritto (contratto individuale e/o altro atto giuridico vincolante)		Art. 83, co. 4 e art. 28 GDPR	Titolare del trattamento	IDEM	
ART. da 25 a 39 GDPR : Art. 29: **mancata istruzione** del Responsabile del procedimento		Art. 83, co. 4 e art. 28 GDPR	Titolare del trattamento	IDEM	
ART. da 25 a 39 GDPR: Art. 30: Mancata adozione del **Registro delle attività di trattamento** da parte del Titolare; Mancata adozione dei Registri delle attività di trattamento dei vari Responsabili		Art. 83, co. 4 e art. 30 GDPR	Titolare e Responsabile del trattamento	IDEM	
ART. da 25 a 39 GDPR: Art. 31: Mancata cooperazione con l'Autorità di controllo		Art. 83, co. 4 e art. 31 GDPR	Titolare e Responsabile del trattamento	IDEM	
ART. da 25 a 39 GDPR: Art. 32: Adozione mísure **tecniche ed organizzative adeguate** per la **sicurezza** dei dati		Art. 83, co. 4 e art. 32 GDPR	Titolare e Responsabile del trattamento	IDEM	
ART. da 25 a 39 GDPR : Art. 33: Mancata notifica all'Autorità di		Art. 83, co. 4 e art. 32 GDPR	Titolare e Responsabile del	IDEM	Stessa sanzione è prevista per il Responsabile se in tali casi non

controllo di una violazione dei dati personali		da 25 a 39	trattamento		informa il Titolare
ART. da 25 a 39 GDPR: Art. 34: Mancata comunicazione all'interessato di una violazione dei dati personali		Art. 83, co. 4 e art. 34 GDPR	Titolare del trattamento	IDEM	La comunicazione è necessaria solo se comporta un "rischio elevato"
ART. da 25 a 39 GDPR: Art. 35: **Mancata valutazione dell'impatto** sulla protezione dei dati		Art. 83, co. 4 e art. 35 GDPR	Titolare del trattamento	IDEM	Si deve effettuare solo se il trattamento presenta un rischio elevato" e in determinati casi specifici. L'Autorità di controllo redige l'elenco delle tipologie di trattamento soggetti a valutazione di impatto
ART. da 25 a 39 GDPR : Art. 36: Mancata **consultazione preventiva** dell'Autorità di controllo qualora la valutazione dell'impatto indichi un "rischio elevato"sulla protezione dei dati		Art. 83, co. 4 e art. 36 GDPR	Titolare e Responsabile del trattamento	IDEM	
ART. da 25 a 39 GDPR : Art. 37: Mancata designazione del **Responsabile della Protezione** dei dati.		Art. 83, co. 4 e art. 37 GDPR	Titolare e Responsabile del trattamento	IDEM	Più amministrazioni pubbliche possono nominare un unico Responsabile della Protezione
ART. da 25 a 39 GDPR : Art. 38 e 39: violazione		Art. 83, co. 4 e art. 38 GDPR	Titolare e Responsabile del	IDEM	

delle norme sullo status e doveri del Responsabile della Protezione			Trattamento + Responsabile della Protezione dei dati		
ART. 42 GDPR : Falsa comunicazioni all'organismo di certificazione per ottenere la certificazione		Art. 83, co. 4 e art. 42 GDPR	Titolare e Responsabile del Trattamento	IDEM	La certificazione è **volontaria**
ART. 43 GDPR : violazione, da parte degli organismi di certificazione, degli obblighi a loro carico		Art. 83, co. 4 e art. 43 GDPR	Organismo di certificazione	IDEM	
ART. 41, co. 4 GDPR : Mancato controllo, da parte dell'organismo di certificazione, della conformità di un trattamento con un codice di condotta		Art. 83, co. 4 e art. 41, co.4	Organismo di certificazione	IDEM	Tutto l'art 43 **non si applica** alle autorità pubbliche e agli **organismi pubblici**
ART. 5 e 6 GDPR : Violazione dei seguenti principi: liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità riservatezza		Art. 83, co. 5 e art. 5 e 6 GDPR	Titolare del Trattamento	Sanzione amministrativa pecuniarie **fino a 20.000.000 EUR,** o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	
ART. 7 GDPR: violazione delle norme sul **consenso** e sulla		Art. 83, co. 5 e art. 7 GDPR	Titolare del Trattamento	IDEM	

sua revoca					
ART. 9 GDPR : violazione del divieto di trattare **dati sensibili e supersensibili** al di fuori dei casi consentiti dallo stesso art. 9		Art. 83, co. 5 e art. 9 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 12, 13 e 14 GDPR : Violazione delle norme sulla **trasparenza** e sugli obblighi di **informazione**, sul diritto di **accesso** dell'interessato, delle informazioni sul consenso e la sua revoca, etc.		Art. 83, co. 5 e art. 12 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 15 GDPR : Violazione delle norme sul diritto di **accesso** dell'interessato, delle informazioni sul consenso e la sua revoca		Art. 83, co. 5 e art. 15 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 16 GDPR: Violazione delle norme sul diritto di **rettifica e cancellazione dei dati**		Art. 83, co. 5 e art. 16 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 17 GDPR: Violazione delle norme sul **diritto all'oblio** (diritto alla cancellazione dei dati)		Art. 83, co. 5 e art. 17 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 18 GDPR: Violazione delle norme sul **diritto alla limitazione** del trattamento		Art. 83, co. 5 e art. 18 GDPR	Titolare e Responsabile del Trattamento	IDEM	

ART. 19 GDPR : Violazione dell'obbligo di notifica in caso di rettifiche, cancellazione o limitazioni e per casistiche specifiche		Art. 83, co. 5 e art. 19 GDPR	Titolare del Trattamento	IDEM	
ART. 20 GDPR : Violazione del **diritto alla portabilità** dei dati		Art. 83, co. 5 e art. 20 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 21 GDPR : Violazione del **diritto di opposizione**		Art. 83, co. 5 e art. 21 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 22 GDPR : Violazione del diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione		Art. 83, co. 5 e art. 22 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 44/49 GDPR : Violazione delle norme in materia di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale		Art. 83, co. 5 e art. 44/49 GDPR	Titolare e Responsabile del Trattamento	IDEM	
CAPO IX – Art. 85/91 GDPR : Violazione delle norme in materia di: A) libertà d'espressione e di informazione; B)		Art. 83, co. 5 e art. 85/91 (Capo IX) GDPR	Titolare e Responsabile del Trattamento	IDEM	

diritto di accesso; C) numero di identificazione personale; D) privacy nel rapporto di lavoro; E) trattamenti per ricerca scientifica, storia o statistica					
Art. 58, co. 1 e GDPR 2 : negare l'accesso all'Autorità di controllo o non osservare un ordine, una limitazione o una sospensione di flusso di dati emanato dall'Autorità di controllo		Art. 83, co. 5 e art. 58 GDPR	Titolare e Responsabile del Trattamento	IDEM	
ART. 83, co. 7: per quanto riguarda gli **organismi pubblici**, **ogni Stato membro può** adottare norme che dispongono **SE** e in quale **MISURA** possono essere inflitte la **sanzioni** amministrative pecuniarie					
Art. 84: Ogni Stato membro stabilisce le norme per altre sanzioni per violazione del Regolamento diverse da quelle amministrative pecuniarie.					

TUTELE

TIPOLOGIA (amministrativa, penale, civile)	**NORMATIVA D.lgs. 196/2003**	**NORMATIVA Reg. UE 679/2016**	**NOTE**	**VARIE**
Sanzioni **PENALI**		n. 149 dei Considerande: spetta a ciascuno Stato prevedere tali sanzioni per le violazioni del presente Regolamento		
Sanzioni **AMMINISTRATIVE PECUNIARIE**		n. 150 dei Considerande: La competenza ad applicarle è dell'Autorità di controllo del singolo Stato membro		
Sanzioni **CIVILI** per il RISARCIMENTO DEL DANNO		Spetta agli organi giurisdizionali interni, secondo le normative dei singoli Stati (da oi Giudice civile)		

Contro le decisioni vincolanti del Comitato ciascuna Autorità di controllo di ciascuno Stato può avanzare **impugnazione** innanzi alla **Corte di Giustizia** (v. n. 143 del Consideranda); stessa cosa può fare qualsiasi persona fisica o giuridica.				