ALLEGATO A ALLA D.G.M. N._____ DEL _____

MANUALE PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679

relativo alla protezione delle persone fisiche

con riguardo al trattamento dei dati personali

Sommario

Art. 1 – Oggetto

1. Il presente Manuale per l'attuazione del Regolamento UE 2016/679 (*General Data Protection Regulation* del 27 aprile 2016 n. 679, di seguito **GDPR** o **Regolamento**), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, d'ora innanzi "**manuale**", ha per oggetto misure procedimentali e regole di dettaglio, ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento comunitario, nonché alla libera circolazione di tali dati, nel Comune di Bisceglie

Art. 2 – Titolare del trattamento

1. Il Comune di Bisceglie, rappresentato, per i fini previsti dal GDPR, dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali (di seguito **Titolare**), raccolti in banche dati, automatizzate o cartacee.
2. Il Titolare è responsabile del rispetto dei principi, applicabili al trattamento di dati personali, stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento di dati personali è effettuato in modo conforme al GDPR.

   Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli dal 15 al 22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

   Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di PEG, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
4. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.
5. Nel caso in cui un tipo di trattamento, specie nel caso di trattamenti effettuati mediante l'uso di tecnologie ICT, possa presentare un rischio elevato per i diritti e le libertà delle persone

fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito **DPIA**) ai sensi dell'art. 35 GDPR, considerando la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, e tenuto conto di quanto indicato dal successivo art. 9.

6. Il Titolare provvede, inoltre, a:
   a) designare i Responsabili del trattamento nelle persone dei Dirigenti/Responsabili P.O. e dei Funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;
   b) nominare il Responsabile della protezione dei dati;
   c) nominare quali Responsabili del trattamento i soggetti pubblici o privati, affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune per la realizzazione di attività connesse alle attività istituzionali, in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge;
   d) predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo nella apposita sezione Amministrazione Trasparente/Altri Contenuti/Privacy del sito istituzionale e aggiornandolo periodicamente; ciascun Responsabile potrà nominare un «sub responsabile» del trattamento, in relazione a un particolare trattamento o a una particolare qualità di dati.
   e) predisporre l'elenco dei dipendenti addetti al trattamento, che saranno definiti «autorizzati al trattamento», i quali devono essere autorizzati al trattamento loro affidato previo apposita formale autorizzazione.

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti e organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità e i mezzi del trattamento, si realizza la **contitolarità** del trattamento (art. 26 GDPR). L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando quanto eventualmente stabilito dalla normativa specificatamente applicabile.

8. Il Comune di Bisceglie favorisce l'adesione a **codici di condotta** elaborati da associazioni e da organismi di categoria rappresentativi, ovvero a iter opportunamente approvati di certificazione della protezione dei dati, al fine di contribuire alla corretta applicazione del GDPR

e, allo stesso tempo, per dimostrare il concreto rispetto del Regolamento da parte del Titolare e dei Responsabili del trattamento.

Art. 3 – Finalità del trattamento

1. Il Comune di Bisceglie effettua i trattamenti per le finalità di seguito descritte:
   a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; rientrano in questo ambito i trattamenti compiuti per:
      - l'esercizio delle funzioni amministrative che riguardano la popolazione e il territorio, nei settori organici dei servizi alla persona e alla comunità, dell'assetto e della utilizzazione del territorio e dello sviluppo economico;
      - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
      - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate 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.

Art. 4 – Responsabile del trattamento

1. I Dirigenti e i Responsabili P.O. delle strutture in cui si articola l'organizzazione dell'Ente sono nominati "Responsabile del trattamento" di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Ciascun Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità e affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6, volte a garantire che i trattamenti siano effettuati in conformità al GDPR.
2. I dipendenti del Comune, Responsabili del trattamento, sono designati mediante decreto di incarico del Sindaco, nel quale sono disciplinati tassativamente:
   - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento e le categorie di interessati;

- gli obblighi e i diritti del Titolare del trattamento.

3. Il Titolare può designare responsabili del trattamento soggetti pubblici o privati, che forniscano le garanzie di cui al comma 1, mediante la stipula di idonei atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

4. Gli atti che disciplinano il rapporto tra il Titolare e i Responsabili del trattamento devono prevedere quanto prescritto dall'art. 28, p.to 3, GDPR; tali atti potranno anche basarsi, su clausole contrattuali "tipo", eventualmente adottate dal Garante per la protezione dei dati personali ovvero dalla Commissione europea.

5. Il Titolare può avvalersi, per il trattamento di dati, anche dei dati c.d. "*particolari*", di soggetti pubblici o privati.

6. E' consentita a ciascun Responsabile del trattamento la nomina di sub-responsabili, per specifiche attività di trattamento, nel rispetto dei medesimi obblighi contrattuali che legano il Titolare e il Responsabile; le operazioni di trattamento possono essere effettuate solo da soggetti opportunamente «autorizzati al trattamento», che operano sotto la diretta autorità del Responsabile, attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.
   Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del 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 e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

7. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità e abbia accesso a dati personali sia in possesso di apposita formazione e istruzione e si sia impegnato alla riservatezza o abbia un adeguato obbligo legale di riservatezza.

8. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, e, in particolare:
   - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
   - all'adozione di idonee misure tecniche e organizzative, adeguate per garantire la sicurezza dei trattamenti;
   - alla sensibilizzazione e alla formazione del personale che partecipa ai trattamenti e alle attività di controllo;
   - ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei

dati (di seguito DPIA) fornendo allo stesso ogni informazione di cui è in possesso;

- a informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che lo stesso Titolare ritenga probabile che, dalla avvenuta violazione dei dati, possano scaturire rischi per i diritti e le libertà degli interessati.

Art. 5 – Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "**DPO**") potrà essere individuato fra i dipendenti del Comune di qualifica non inferiore alla cat. D (oppure C), purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione comunale. Il Titolare ed il Responsabile del trattamento provvedono affinché il DPO mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

2. Nel caso in cui il DPO non sia un dipendente dell'Ente, potrà essere designato un soggetto giuridico, selezionato mediante le procedure ordinarie di selezione proprie della pubblica amministrazione.

   Il soggetto giuridico designato deve possedere le medesime qualità professionali richieste al dipendente dell'ente, deve aver maturato approfondita conoscenza del settore e delle strutture organizzative degli enti locali, nonché delle norme e procedure amministrative agli stessi applicabili; i compiti attribuiti al DPO saranno indicati in apposito contratto di servizi. Nel caso di nomina di un soggetto esterno, il DPO esterno è tenuto a indicare una persona fisica che lo rappresenti nell'incarico e che sia individuato quale referente per il Titolare/Responsabile: il nominativo sarà, altresì, comunicato al Garante nella apposita "*Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati*" (art.37, par.7 del Regolamento (UE) 2016/679 - GDPR e art. 28, c. 4 del D.Lgs. 51/2018). Il soggetto affidatario dovrà mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare e al Responsabile del trattamento.

3. Il DPO è incaricato dei seguenti compiti:
   a) *informare e fornire consulenza* al Titolare e al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. Il DPO può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit*, interno o

esterno, in materia di protezione dei dati, può indirizzare le attività di formazione per il personale autorizzato al trattamento dei dati personali, e a quali trattamenti dedicare maggiori risorse in relazione al rischio riscontrato;

b) *sorvegliare l'osservanza del GDPR* e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) *sorvegliare* sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) *fornire*, se richiesto, *un parere in merito alla valutazione di impatto sulla protezione dei dati* (DPIA) e sorvegliarne lo svolgimento.

   Il Titolare si consulta con il DPO in merito:

   - alla necessità di condurre una DPIA;
   - quale metodologia adottare nel condurre una DPIA;
   - se condurre la DPIA utilizzando risorse interne o esterne;
   - quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
   - al giudizio se la DPIA sia stata condotta correttamente e se le conclusioni raggiunte nel corso della valutazione del rischio siano conformi al GDPR (e, pertanto, decidere se procedere con il trattamento e quali salvaguardie applicare);

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR. A tali fini il nominativo del DPO è comunicato dal Titolare del trattamento al Garante;

f) altri compiti e funzioni, a condizione che il Titolare, o il Responsabile del trattamento, si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

4. Il Titolare e il Responsabile del trattamento assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

   - il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili di P.O. che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
   - il DPO deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza

idonea, scritta od orale;

- il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tale decisione;
- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

5. Nello svolgimento dei compiti affidatigli il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il DPO:
   a) procede a una mappatura delle aree di attività, valutandone il grado di rischio in termini di protezione dei dati;
   b) definisce un ordine di priorità nell'attività da svolgere – redigendo un piano delle attività da comunicare al Titolare e ai Responsabili del trattamento – incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati.
6. Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.
7. La figura di DPO è incompatibile con chi determina le finalità o i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
   - il Responsabile per la prevenzione della corruzione e per la trasparenza;
   - il Responsabile del trattamento;
   - qualunque incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.
8. Il Titolare e i Responsabili del trattamento forniscono al DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al DPO:
   - supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di PEG e di Piano della performance;
   - nel caso il DPO sia interno, tempo sufficiente per l'espletamento dei compiti affidati al DPO;
   - supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale; è auspicabile (in relazione alle capacità organizzative dell'Ente) la costituzione di un gruppo di lavoro, di cui fa parte lo stesso

DPO;

- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

9. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.
   Il DPO non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.
   Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.
   Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art. 6 – Sicurezza del trattamento

1. Il Regolamento europeo per la protezione dei dati personali impone al titolare del trattamento l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti. L'articolo 25, in particolare, introduce i principi di "*privacy by design*" e "*privacy by default*", un approccio concettuale innovativo che impone l'obbligo di prevedere , preliminarmente alla esecuzione del trattamento, gli strumenti e le corrette impostazioni a tutela dei dati personali.
   L'adozione di adeguate misure di sicurezza, in riferimento ai principi di protezione dei dati fin dalla progettazione (*by design*) e di protezione per impostazione predefinita (*by default*) è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche.
   Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.
2. Il **Comune di Bisceglie**, e ciascun **Responsabile del trattamento**, mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di

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

L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento, che derivano, in particolar modo, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. La protezione efficace dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

3. Le misure tecniche e organizzative di sicurezza finalizzate alla riduzione dei rischi connessi al del trattamento dei dati personali ricomprendono:
   a. la pseudonimizzazione dei dati personali;
   b. la minimizzazione dei dati personali;
   c. la cifratura dei dati personali;
   d. la capacità di assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
   e. la capacità di ripristinare tempestivamente, in caso di incidente, fisico o tecnico, la disponibilità dei dati e l'accesso agli stessi;
   f. la definizione di una procedura in grado di testare, verificare e valutare, con regolarità, l'efficacia delle misure tecniche e organizzative, al fine di garantire la sicurezza del trattamento.

4. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:
   a. sistemi di autenticazione;
   b. sistemi di autorizzazione;
   c. sistemi di protezione (antivirus; firewall; antintrusione; altro);
   d. misure antincendio;
   e. sistemi di rilevazione di intrusione;
   f. sistemi di sorveglianza;
   g. sistemi di protezione con videosorveglianza;
   h. registrazione accessi;
   i. porte, armadi e contenitori dotati di serrature e ignifughi;
   j. sistemi di copiatura e conservazione di archivi elettronici;
   k. altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

5. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o a un meccanismo di certificazione approvato.
6. Il Comune di Bisceglie, e ciascun Responsabile del trattamento, si obbliga a impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto e abbia accesso a dati personali.
7. I nominativi e i dati di contatto del Titolare, dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "*privacy*", eventualmente già presente.
8. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).

Art. 7 – Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a. il nome e i dati di contatto del Comune, del Sindaco e/o del suo Delegato ai sensi del precedente art.2, eventualmente del Contitolare del trattamento, del DPO;
   b. le finalità del trattamento;
   c. la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e. l'eventuale trasferimento di dati personali verso un paese terzo o verso una organizzazione internazionale;
   f. ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g. il richiamo alle misure di sicurezza tecniche e organizzative del trattamento adottate, in riferimento al precedente art. 6.
2. Il Registro è tenuto dal Titolare, ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea, secondo lo schema di cui all'**Allegato A** al presente **manuale**; nello stesso possono essere inserite ulteriori informazioni, tenuto conto delle scelte organizzative dell'Ente.
3. Il Titolare del trattamento può decidere di affidare al DPO il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.
4. Con riferimento alla dimensioni organizzative dell'Ente, costituito in un unico AOO, il Titolare potrà decidere di redigere e tenere un Registro unico dei trattamenti, contenente le

informazioni di cui ai commi precedenti e quelle di cui al successivo art. 8, sostituendo entrambe le tipologie di registro dagli stessi disciplinati, secondo lo schema di cui all'**Allegato C** al presente **manuale**. Nella predetta circostanza, il Titolare può delegare la tenuta del registro a un solo Responsabile del trattamento, ovvero può decidere di affidare tale compito al DPO, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha, comunque, la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Art. 8 – Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile di cui al precedente art. 4, reca le seguenti informazioni:
   a. il nome e i dati di contatto del Responsabile del trattamento e del DPO;
   b. le categorie di trattamenti effettuati da ciascun Responsabile:
      i. raccolta; ii. registrazione; iii. organizzazione; iv. strutturazione; v. conservazione; vi. adattamento o modifica; vii. estrazione; viii. consultazione; ix. uso; x. comunicazione; xi. raffronto; xii. interconnessione; xiii. limitazione; xiv. cancellazione; xv. distruzione; xvi. profilazione; xvii. pseudonimizzazione; ogni altra operazione applicata a dati personali;
   c. l'eventuale trasferimento di dati personali verso un paese terzo o una organizzazione internazionale;
   d. il richiamo alle misure di sicurezza tecniche e organizzative del trattamento adottate, in riferimento a quanto indicato dal precedente art. 6.
2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema di cui all'**Allegato B** al presente **manuale**.
3. Il Responsabile del trattamento può decidere di affidare al DPO il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

Art. 9 – Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie nel caso in cui preveda l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, tenendo in debita considerazione la natura,

l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione circa la necessità di effettuare la DPIA, si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione, redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, p.ti da 4 a 6, GDPR.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p.to 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a. trattamenti valutativi o di *scoring*[1], compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato
   b. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
   c. monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
   d. trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
   e. trattamenti di dati su larga scala, tenendo conto:
      i. del numero di numero di soggetti interessati dal trattamento
      ii. del rapporto,in termini numerici o di percentuale, in relazione alla popolazione di riferimento
      iii. del volume dei dati e/o dell'ambito delle diverse tipologie di dati oggetto di trattamento
      iv. della durata o persistenza dell'attività di trattamento
      v. dell'ambito geografico dell'attività di trattamento
   f. combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
   g. trattamento di dati relativi a interessati vulnerabili, in quanto il trattamento relativo ai dati di un "interessato" particolarmente vulnerabile è meritevole di specifica tutela in quanto per un tale soggetto può verificarsi una situazione di disequilibrio nel rapporto con il Titolare del

1 Lo **scoring** è un sistema di "classificazione" di un "interessato", che utilizza complessi algoritmi, capaci di prendere in considerazione un gran numero di variabili relative alla soggetto "interessato"al fine di stilare una posizione di classifica dello stesso soggetto, in relazione a affidabilità, risk management, registrazione dei dati. Questo modo di procedere determina l'importante vantaggio in riferimento a eventuali decisioni da prendere in relazione al soggetto, ancorate a criteri quanto più possibile "oggettivi", riducendo così la possibilità di errori o inesattezze.

trattamento (dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori);

h. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i. tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che il trattamento non possa presentare un rischio elevato: Allo stesso modo, il Titolare può motivatamente ritenere che anche per un trattamento che soddisfa solo uno dei criteri di sopra indicati, sia comunque necessaria la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA a un altro soggetto, interno o esterno al Comune.
   Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA.
   Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA, fornendo ogni informazione necessaria.
   Il responsabile della sicurezza dei sistemi informativi (ovvero l'amministratore di sistema), se nominato, e/o l'ufficio competente per i sistemi ICT, forniscono, anche mediante l'assistenza di fornitori esterni, supporto al Titolare per lo svolgimento della DPIA.
5. Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
   Il responsabile della sicurezza dei sistemi informativi (ovvero l'amministratore di sistema), se nominato, e/o l'ufficio competente per i sistemi ICT, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza o operative.
6. La DPIA non è necessaria nei casi seguenti:
   - ✓ se il trattamento non comporta un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p.to 1, GDPR;
   - ✓ se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA; in tal caso si possono utilizzare i risultati della DPIA svolta in precedenza per l'analogo trattamento;
   - ✓ se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;

- ✓ se un trattamento trova la propria base legale nella vigente legislazione, che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano stati oggetto di verifica preliminare da parte del Garante della Privacy, o da un RDP, precedentemente all'entrata in vigore del GDPR, e che proseguano con le stesse modalità oggetto della accennata verifica. Occorre, inoltre, tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non saranno modificate, sostituite o abrogate.

7. La DPIA deve essere condotta, prima di dar luogo al trattamento:
   a) mediante l'implementazione di processi:
      i) di descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati;
      ii) di descrizione dei dati personali oggetto del trattamento, dei destinatari e del periodo previsto di conservazione dei dati stessi;
      iii) di descrizione funzionale del trattamento;
      iv) di descrizione funzionale degli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
   b) mediante la valutazione della necessità e proporzionalità dei trattamenti, sulla base:

i. delle finalità specifiche, esplicite e legittime	ii. della liceità del trattamento	iii. dei dati adeguati, pertinenti e limitati a quanto necessario
iv. del periodo limitato di conservazione	v. dell'ambito geografico dell'attività di trattamento	delle informazioni fornite agli interessati
vi. del diritto di accesso e portabilità dei dati	vii. del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento	viii. dei rapporti con i responsabili del trattamento
ix. delle garanzie per i trasferimenti internazionali di dati	x. consultazione preventiva del Garante privacy	

   c) mediante la valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati; devono essere determinati l'origine, la natura, la particolarità e la gravità dei rischi o, più specificatamente, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
   d) mediante l'individuazione delle misure previste per affrontare e attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR,

tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
9. Il Titolare, ai sensi dell'art. 36 del GDPR, deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale e alla sanità pubblica.
10. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.
11. Una sintesi delle principali risultanze del processo di valutazione eventualmente effettuato è pubblicata sul sito istituzionale dell'Ente, nella apposita sezione "privacy".

Art. 10 – Violazione dei dati personali

1. Per violazione dei dati personali ("*data breach*") si intende la violazione di sicurezza che comporta accidentalmente, o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.
2. Il Titolare, qualora ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e, comunque, senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato a informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti a una violazione, in conformità al considerando 75 del GDPR, sono di seguito riportati:
   - danni fisici, materiali o immateriali alle persone fisiche;
   - perdita del controllo dei dati personali;
   - limitazione dei diritti ovvero discriminazione;
   - furto o usurpazione d'identità;

- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari, etc.).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare gli interessati, senza ingiustificato ritardo, con un linguaggio semplice e chiaro, al fine di fare comprendere loro la natura della violazione dei dati personali che si è verificata.
   I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   - riguardare categorie *particolari* di dati personali;
   - comprendere dati che possono accrescere ulteriormente i potenziali rischi (dati di localizzazione, dati finanziari, dati relativi ad abitudini e preferenze);
   - comportare rischi imminenti e con un'elevata probabilità di accadimento (rischio di perdita finanziaria in caso di furto di dati relativi a sistemi digitali di pagamento);
   - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (utenti deboli, minori, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 GDPR; la comunicazione all'interessato deve contenere, almeno, le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d.
6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze a esse relative, le conseguenze e i provvedimenti adottati, o che intende adottare, per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza, in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

Art.11 – Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del GDPR e tutte le sue norme attuative vigenti (Direttiva 2016/680; DPR 15 gennaio 2018, n. 15; D.Lgs. 18 maggio 2018, n. 51; D.Lgs. 10 agosto 2018, n. 101).
2.

ALLEGATO A – SCHEMA DI REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

REGISTRO ATTIVITA' DI TRATTAMENTO (art. 30, c.1, GPRD)

ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

	TRATTAMENTO			DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Contitolare (eventuale Rappres.nte)	Categoria	Dati sensibili (SI/NO)	Termine ultimo cancell.ne	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) (SI/NO)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

ALLEGATO B – SCHEMA DI REGISTRO DELLE CATEGORIE DI ATTIVITÀ DI TRATTAMENTO

REGISTRO CATEGORIE DI ATTIVITA' DI TRATTAMENTO (art. 30, c.2, GPRD)			
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile del trattamento**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
		Registro tenuto da	
		Data di creazione	
		Ultimo aggiornamento	
		N. schede compilate	
		Prossima revisione	

	TRATTAMENTO				TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Categorie	eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

ALLEGATO C – SCHEMA DI REGISTRO UNICO DEI TRATTAMENTI

REGISTRO UNICO DEI TRATTAMENTI (art. 7, c.8, Regolamento comunale)			
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

	TRATTAMENTO					DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Categorie	eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte)	Responsabile	Categoria	Dati sensibili (SI/NO)	Termine ultimo cancell.ne	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) (SI/NO)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

GLOSSARIO

Ai fini del presente MANUALE, si intende:

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, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Titolare del trattamento

Il Comune, che singolarmente, o insieme ad altre autorità pubbliche o ad altro ente locale, persona fisica o giuridica, autorità pubblica, servizio o altro organismo determina finalità e mezzi del trattamento di dati personali.

Responsabile del trattamento

Il Dirigente/Responsabile P.O., oppure la persona fisica o giuridica, il professionista privato o impresa esterna, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Sub-Responsabile del trattamento

Il dipendente della struttura organizzativa del Comune, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, all'uopo delegata, in forma scritta, dal Responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento.

Responsabile per la protezione dati – DPO

Il dipendente della struttura organizzativa del Comune (titolare del trattamento), il professionista privato o impresa esterna (ovvero un dipendente di essa) o del responsabile del trattamento, designato, dal Titolare del trattamento, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
Il responsabile della protezione dei dati assolve i suoi compiti sulla base di un contratto di servizio, ovvero di altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, in cui sono disciplinati obblighi e doveri

Registri delle attività di trattamento

Elenchi dei trattamenti tenuti, secondo le rispettive competenze, dal Titolare o dal Responsabile del trattamento, in forma cartacea o telematica. Il documento dovrà contenere, come statuito dall'art. 30 del GDPR, una serie di informazioni sulle attività riguardanti il trattamento dei dati.

DPIA – Data Protection Impact Assessment[2]

E' una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

Garante Privacy

Il c.d. Garante Privacy (*garante per la protezione dei dati personali*) è un'autorità amministrativa indipendente istituita dalla Legge 31 dicembre 1996, n. 675, successivamente disciplinata dal "*Codice in materia di protezione dei dati personali*" (d.lg. 30 giugno 2003 n. 196).

2 Valutazione d'impatto sulla protezione dei dati

In riferimento alla REDAZIONE DEI REGISTRI inerenti ai trattamento dei dati, si intende:

Categorie di trattamenti

Un elenco non esaustivo delle possibili categorie di trattamenti è di seguito riportato: raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto o interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

Categorie di dati personali

Dalla definizione di «**dato personale**», ai sensi dell'art. 4 GDPR- "qualsiasi informazione riguardante una persona fisica (**interessato**), identificata o identificabile scaturisce che un elenco non esaustivo delle possibili categorie di dati personali è di seguito riportato: dati identificativi quali cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale; dati inerenti allo stile di vita; dati concernenti la situazione economica, finanziaria, patrimoniale, fiscale; dati relativi alle connessioni, così come rilevati degli ISP (indirizzo IP, login, ecc.); dati di localizzazione (ubicazione, GPS, GSM, ecc.).

Finalità del trattamento

Il principio di finalità (o limitazione della finalità) dei dati prevede che un trattamento di dati personali sia legittimo in relazione al fine del trattamento stesso.
I dati devono essere raccolti per finalità determinate, esplicite e legittime, e, pertanto, devono essere trattati secondo modalità compatibili con la finalità assunta. Stabilire gli scopi del trattamento, e esplicitarli nelle comunicazioni all'interessato, aiuta a comprendere ciò che è davvero necessario e non raccogliere dati superflui.
Per quanto concerne gli Enti Locali possono essere individuate come *finalità del trattamento* l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri: funzioni amministrative inerenti alla popolazione e al territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto e della utilizzazione del territorio e dello sviluppo economico; la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica; l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune.
Gli adempimenti di un obbligo legale al quale è soggetto il Comune ovvero l'esecuzione di un contratto con i soggetti interessati.
Altre specifiche e diverse finalità.

Misure tecniche e organizzative

Il GDPR richiede l'adozione, da parte del titolare del trattamento, di *misure tecniche* e di *misure organizzative* adeguate al rischio per i diritti e le libertà degli interessati.
Spesso si identifica questo requisito con le sole misure di sicurezza tecnologiche (finalizzate alla *cyber security*) che, tuttavia, rappresentano solo una parte dell'intero complesso di misure che il GDPR chiede di adottare per tutelare i dati personali degli interessati.
Secondo gli standard ISO 27001, più "prossimi" alle istanze sollecitate dalle attività di *data protection*, si intendono per *misure organizzative* tutte quelle politiche, procedure, regolamenti idonei ad ottenere un livello di sicurezza e protezione delle informazioni (dei dati) coerente con gli obiettivi e le strategie dell'organizzazione.
Rappresentano, per esempio, misure organizzative quelle che:

- ☑ prevedono la separazione dei compiti;
- ☑ contemplano ed individuano ruoli e responsabilità;
- ☑ permettono la gestione degli utenti, dei loro diritti, degli accessi fisici;
- ☑ consentono la rintracciabilità, la misurazione, i controlli e le verifiche;
- ☑ sono finalizzate alle gestione degli asset e dei supporti rimovibili;
- ☑ promuovono l'istruzione e la promozione della consapevolezza.

Un elenco non esaustivo delle possibili *misure tecniche e organizzative*, adeguate al rischio di trattamenti, è di seguito riportato:

- ☑ pseudonimizzazione; minimizzazione; cifratura
- ☑ misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei

sistemi e dei servizi che trattano i dati personali
- ☑ procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative, al fine di garantire la sicurezza del trattamento – e altre misure specifiche adottate per il particolare trattamento in questione
- ☑ sistemi di autenticazione
- ☑ sistemi di autorizzazione
- ☑ sistemi di protezione (antivirus; firewall; antintrusione; ecc.) – adottati per lo specifico trattamento ovvero per il Servizio/Ente nel suo complesso.
- ☑ misure antincendio;
- ☑ sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza;
- ☑ registrazione accessi;
- ☑ porte, armadi e contenitori dotati di serrature;
- ☑ sistemi di copiatura e conservazione archivi elettronici;
- ☑ altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico – adottati per lo specifico trattamento ovvero per il Servizio/Ente nel suo complesso.
- ☑ procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Dati sensibili

Ai sensi del D.Lgs. 196/2003, c.d. codice privacy, erano considerati dati sensibili quei dati personali atti a rivelare:
- ☑ l'origine razziale ed etnica di un individuo;
- ☑ le sue convinzioni e adesioni religiose, politiche e filosofiche;
- ☑ lo stato di salute e la vita sessuale.

Questi dati godevano di maggior tutela e il loro trattamento era consentito solo previo il consenso scritto dell'interessato.

Nel General Data Protection Regulation non vi è il concetto di dati sensibili ma di dati particolari e all'articolo 9 recita: "*È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*" Il divieto non si applica in presenza di consenso esplicito o di necessità per assolvere gli obblighi.

Categorie di interessati

Cittadini residenti; minori di anni 16; elettori; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; ecc.

Categorie di destinatari

Persone fisiche; autorità pubbliche e altre PA; persone giuridiche private; altri soggetti.