Regolamento Comunale per l'attuazione del
Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Art. 1

Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio finalizzate alla migliore funzionalità ed efficacia dell'attuazione, nel Comune di Piedimulera del Regolamento europeo (Regolamento Generale Protezione Dati del 27 aprile 2016 n. 679 del Parlamento Europeo e del Consiglio, di seguito indicato con "GDPR", *"General Data Protection Regulation"*), relativo alla protezione delle persone fisiche con riguardo al trattamento ed alla libera circolazione dei dati personali.

Art. 2

Titolare del trattamento

1. Comune di Piedimulera rappresentato ai fini previsti dal GDPR dal Sindaco *pro tempore*, è il Titolare del trattamento (di seguito indicato con "Titolare") dei dati personali, raccolti o meno in archivi, automatizzati o cartacei, come definiti dall'art. 4, paragrafo 1, n. 6 GDPR. Il Sindaco può delegare le relative funzioni ai Responsabili dei Servizi / Posizioni.Organizzative in possesso di adeguate competenze, quali persone autorizzate al trattamento dati.
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 ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR (art. 24 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 15-22 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 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, ovverosia la persona fisica identificata o identificabile, le seguenti informazioni:

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 siano stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA", *"Data Protection Impact Assessment"*), ai sensi dell'art. 35 GDPR, considerando la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

6. Il Titolare, inoltre, provvede a:

a) Designare le persone autorizzate al trattamento dei dati con deleghe speciali nelle persone dei Responsabili di Servizio/ P.O. e dei funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti negli archivi 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, quale Responsabile del trattamento, la persona fisiche o giuridica, l'autorità pubblica, il servizio o un altro organismo affidatari di attività e servizi per conto dell'Amministrazione Comunale, relativamente alle banche dati gestite da soggetti esterni al Comune, in virtù di convenzioni, di contratti, o di incarichi professionali, o di altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 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 ed alle rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare.

Art. 3

Finalità del trattamento

1. I trattamenti sono leciti ai sensi dell'art. 6 GDPR e 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:

- l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale, affidate 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) Specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 4

Responsabile del trattamento

1. Il Titolare può avvalersi, per il trattamento di dati, anche particolari ai sensi dell'art. 9 GDPR, di persone fisiche o giuridiche, autorità pubbliche, servizi o altri organismi, che, in qualità di Responsabili del trattamento (art. 28 GDPR), forniscano garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e

organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR, stipulando 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.

2. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, paragrafo 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali, oppure dalla Commissione europea.

3. È consentita, ex art. 28, paragrafi 2 e 4 GDPR, la nomina di sub-responsabili da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali, ex art. 28, paragrafo 3 GDPR, che legano il Titolare ed il Responsabile primario, previa autorizzazione scritta, specifica o generale del Titolare stesso.

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 adeguatamente sull'operato del sub-responsabile.

4. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza (art. 29 GDPR).

5. 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, ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare (art. 30, paragrafo 2, GDPR);
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti (art. 32 GDPR);
- all'istruzione e alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo (art. 29 GDPR);
- alla designazione del Responsabile per la Protezione dei Dati (DPO), qualora sia necessario ai sensi dell'art. 37 GDPR;
- ad assistere il Titolare nella "DPIA", fornendo allo stesso ogni informazione di cui è in possesso (artt. 35-36 GDPR);

- ad 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 in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati (art. 33 GDPR).

Art. 5

Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "DPO" *Data Protection Officer*), ai sensi dell'art. 37 GDPR, è designato, con apposito atto, in funzione delle qualità professionali ed, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali.
2. Il DPO è incaricato dei seguenti compiti *ex* art. 39 GDPR:

a) informare e fornire consulenza al Titolare e/o 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. In tal senso, il DPO può indicare al Titolare e/o al Responsabile del trattamento:

- i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati,
- le attività di formazione interna per i dipendenti che trattano dati personali,
- i trattamenti ai quali dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, ferme 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, in particolare, si consulta con il DPO sulle seguenti questioni:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;

- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno,
- se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al GDPR;

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, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini, il nominativo del DPO è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

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

3. Il Titolare ed 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 Responsabili dei Servizi/P.O. che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
- il DPO deve disporre tempestivamente di tutte le informazioni pertinenti alle 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 dal Titolare determini condotte difformi da quelle raccomandate dal DPO, è necessario che essa sia specificamente motivata;
- il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. 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 ad una mappatura delle aree di attività, valutandone il grado di rischio in termini di protezione dei dati;

b) definisce un ordine di priorità nell'attività da svolgere - ovverosia un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

4. 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.

5. La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento.

6. Il Titolare ed il Responsabile 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 Responsabili dei Servizi /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 e di Piano della performance;
- tempo sufficiente per l'espletamento dei suoi compiti;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ufficio o gruppo di lavoro DPO (formato dal DPO stesso e dal rispettivo personale);
- 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.

7. Il DPO opera in posizione di autonomia nello svolgimento dei compiti attribuitigli; in particolare, non deve ricevere istruzioni sulla loro attuazione, né sull'interpretazione e risoluzione di una specifica questione attinente alla normativa sulla 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).

Nel caso in cui siano rilevate dal DPO, o sottoposte alla sua attenzione, decisioni incompatibili con il GDPR e con le indicazioni fornite dal medesimo, è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art. 6

Sicurezza del trattamento

1. Il mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono ai sensi dell'art. 32 GDPR: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Costituiscono misure tecniche ed organizzative che possono essere adottate:
- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4. Il Comune di Piedimulera si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per suo conto ed abbia accesso a dati personali.

I nominativi ed i dati di contatto del Titolare e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, nella sezione Amministrazione trasparente e nella sezione "privacy".

Fino alla eventuale futura modifica/sostituzione/abrogazione del D. Lgs. 196/2003, 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, ai sensi dell'art. 30 GDPR, almeno le seguenti informazioni:

a) il nome ed i dati di contatto del Comune, 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 od una organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

3. 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; nello stesso Registro, possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

Il Titolare può decidere di tenere un Registro unico dei trattamenti che contiene le informazioni di cui ai commi precedenti e quelle di cui al successivo art. 8, sostituendo entrambe le tipologie di registro dagli stessi disciplinati.

Art. 8

Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate dal Comune di Piedimulera nel ruolo di Responsabile del trattamento per conto di un diverso titolare reca le seguenti informazioni:

a) il nome ed i dati di contatto del Responsabile del trattamento, di ogni titolare del trattamento per conto del quale agisce e del DPO;

b) le categorie di trattamenti effettuati: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;

c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

Art. 9

Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede 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 (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. 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, paragrafo 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato sono, secondo le Linee Guida in materia del WP 29 (Gruppo di Lavoro ex articolo 29), i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) le categorie di dati personali particolari e giudiziari di cui agli artt. 9 e 10 GDPR, qualora siano trattate su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle

diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

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

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune. Il Titolare deve sempre consultarsi con il DPO, che monitora lo svolgimento della DPIA. La consultazione dev'essere effettuata anche per assumere la decisione se compiere o meno la DPIA; tali consultazione e conseguente decisione devono essere documentate nell'ambito della DPIA. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono 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, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 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 questo caso, si possono utilizzare i risultati della DPIA svolta 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.
- se taluni trattamenti siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o di un DPO e continuino ad essere condotti con le stesse modalità oggetto di tale verifica; a questo proposito, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. La DPIA è condotta, prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento, dei dati personali oggetto del trattamento, dei destinatari e del periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; descrizione degli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- della consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi

o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il 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 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 ed alla sanità pubblica. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari, tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 10
Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "*data breach*"), conformemente all'art. 33 GDPR, 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, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire senza ingiustificato e, ove possibile, entro 72 ore dal momento dell'avvenuta conoscenza.

3. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

4. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonomizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

5. Se il Titolare ritiene elevato il rischio per i diritti e le libertà degli interessati derivato dalla violazione, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro, al fine consentire loro la comprensione della natura della violazione dei dati personali verificatasi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo esemplificativo:

- 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 (ad esempio, dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio, rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio 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 al citato art. 33 GDPR, come richiamato dall'art. 34, paragrafo 2, GDPR.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza, al fine di essere esibita al Garante Privacy, qualora la richieda per verificare il rispetto delle disposizioni del GDPR.

Art. 11

Rinvio

Per tutto quanto non espressamente disciplinato con il presente Regolamento Comunale, si applicano le disposizioni del GDPR e tutte le sue norme attuative emanate ed emanande.