



UNIONE DEI COMUNI MONTANI COLLINE DEL FIORA

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

Approvato con delibera di Giunta n. 32 del 25/05/2018

Art. 1 - Oggetto
Art. 2 - Titolare del trattamento
Art. 3 - Finalità del trattamento
Art. 4 - Responsabile del trattamento
Art. 5 - Responsabile della protezione dati
Art. 6 - Sicurezza del trattamento
Art. 7 - Registro delle attività di trattamento
Art. 8 - Registro delle categorie di attività trattate
Art. 9 - Valutazione d'impatto sulla protezione dei dati
Art. 10 - Violazione dei dati personali
Art. 11 – Rinvio ed entrata in vigore

Allegati

A) schema di registro attività di trattamento
B) schema di registro categorie attività di trattamento 3

Art. 1 Oggetto

1. La presente disciplina ha per oggetto misure procedurali, organizzative e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nell'Unione di Comuni Montana Colline del Fiora (di seguito "Unione"), ed è da considerarsi quale allegato al vigente Regolamento degli Uffici e dei Servizi (ROUS).

Art.2 Titolare del trattamento

1. L'Unione, rappresentata ai fini previsti dal RGPD dal Presidente pro tempore, è il Titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: 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 RGPD. Le misure sono definite in atti adottati dagli organi dell'Unione sulla base delle competenze definite dallo Statuto e dal ROUS.

4. 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 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

5. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa, 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.

6. Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

7. Nel caso in cui un tipo di trattamento, specie se prevede in particolare 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") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

8. Il Titolare, inoltre, provvede a:

a) designare i Responsabili del trattamento nelle persone dei Titolari di P.O. così come individuati dall'organigramma allegato al vigente ROUS ovvero dai decreti presidenziali di nomina. Essi sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;

b) nominare il Responsabile della protezione dei dati;

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Unione, relativamente alle banche dati gestite da soggetti esterni all'organizzazione dell'Amministrazione in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

9. L'Unione è titolare del trattamento anche per i dati raccolti nell'esercizio associato di funzioni e servizi ad essa assegnati dai Comuni membri in attuazione dello statuto. Nel caso in cui i dati in questione siano raccolti presso i Comuni medesimi, spetta all'Unione provvedere all'informazione di cui all'art. 14 del RGPD in occasione del primo utilizzo. L'interessato può rivolgersi per ottenere informazioni e per la tutela dei propri diritti sia all'Unione che al Comune.

10. Nel caso in cui l'Unione stipuli accordi e convenzioni con altri Comuni ed enti locali per l'esercizio associato di funzioni per le quali è prevedibile la raccolta e l'utilizzo di dati personali, la convenzione disciplina le rispettive responsabilità.

11. Nel caso in cui l'Unione divenga titolare di dati per la gestione di attività affidate 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 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

Art.3 Finalità del trattamento

1. I trattamenti sono compiuti dall'Unione 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, della gestione delle foreste e del patrimonio agroforestale regionale e dello sviluppo economico;

- la gestione dei servizi di statistica;

- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale, regionale e comunale affidate all'Unione 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 soggetta l'Unione. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina; 5

- 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 responsabili interni del trattamento sono designati mediante decreto di incarico del Presidente tra le figure apicali di cui agli articoli 5 e 7 del ROUS dell'Unione che, in caso di assenza o impedimento sono sostituiti a norma degli articoli 6 e 8 del ROUS medesimo. Il decreto di incarico, di norma, fa riferimento ai trattamenti dei dati personali di banche dati ed archivi di competenza di ogni responsabile secondo la ripartizione interna dell'organizzazione come definita dal medesimo ROUS e dei relativi allegati, nonché, ove esistenti, a convenzioni associative con altri enti locali che richiedono il trattamento di dati personali. I responsabili interni del trattamento sono tenuti a procedere al trattamento per le finalità definite dalla legge o da atti del titolare del trattamento, secondo quanto indicato all'articolo 3, e ad assicurare che la durata del trattamento non ecceda le strette necessità derivanti dall'attività amministrativa di competenza, facendo in modo che siano rispettati, gli obblighi e i diritti del titolare del trattamento ed i diritti degli interessati sanciti dal RGPD.

2. I responsabili esterni del trattamento sono soggetti incaricati di rendere servizi all'Unione che richiedono il trattamento di dati personali. Debbono assicurare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD e garantisca la tutela dei diritti dell'interessato. Il contratto principale, o altro atto giuridico equivalente a questo connesso, riporta clausole adeguate per definire puntualmente il contenuto concreto delle disposizioni di cui alle lettere da a) ad h) del paragrafo 3 dell'articolo 28 del RGPD, con particolare riguardo alla durata del trattamento o dei trattamenti assegnati ed alle operazioni da porre in essere al termine della prestazione dei servizi relativi al trattamento, nonché agli obblighi e ai diritti del Titolare.

3. Sulla base dell'ordinamento statutario ed organizzativo dell'Unione, la designazione dei titolari esterni del trattamento è effettuata dai responsabili interni nominati dal Presidente titolare ciascuno in base alla competenza come indicato al comma 1. Resta salva la possibilità del titolare, inteso come organi rappresentativi dell'Unione, di procedere direttamente alla designazione quando l'approvazione dell'atto amministrativo, della convenzione o dell'accordo è di loro competenza in base all'ordinamento vigente.

4. Fermo restando che gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono contenere quanto previsto dall'art. 28, p. 3, RGPD, tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

3. E' consentita la nomina da parte di ciascun Responsabile del trattamento di sub-responsabili del trattamento con atto scritto per specifiche attività di trattamento, previa informazione preventiva al Titolare e nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario.

4. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

5. 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.

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

7. 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;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- 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 che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare 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 "RPD") è individuato in un professionista esterno in possesso delle necessarie capacità professionali scelto tramite adeguata procedura prevista dalla legge.

2. Il RPD individuato dall'Unione può svolgere i propri compiti anche nei confronti dei Comuni membri qualora i rispettivi Sindaci provvedano a nominarlo per tale funzione.

3. Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD 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 il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e 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 RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) eventuale tenuta dei registri di cui ai successivi artt. 7 e 8;

g) 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 RPD.

4. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;

- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

5. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:

a) partecipa alla mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

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

6. Il RPD 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'Unione.

7. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento, in particolare con:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;

- il Responsabile del trattamento;

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

8. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e della Giunta, 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;

- 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 RPD 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.

10. Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

11. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Presidente o suo delegato - od al Responsabile del trattamento.

12. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art.6 Sicurezza del trattamento

1. L'Unione e ciascun Responsabile del trattamento mettono 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: 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 dal Servizio cui è preposto ciascun Responsabile del trattamento:

- 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. Le misure per la sicurezza degli archivi e dei documenti dell'Unione sono comprese nel Manuale per la gestione del protocollo e dei flussi documentali, adottato con deliberazione della Giunta esecutiva n. 31 del 21/04/2017.

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 ad un meccanismo di certificazione approvato.

6. L'Unione e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

7. I nominativi ed i dati di contatto del Titolare e dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'Unione, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente 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. 196/2003).

Art.7 Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni di cui all'articolo 30 del RGPD.

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 dell'Unione in forma telematica/cartacea, secondo lo schema allegato A al presente disciplinare.
3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.
4. Il formato del registro di cui al comma 2 può essere variato con atto del Presidente per esigenze organizzative, fermo restando il contenuto minimo delle informazioni richieste dal RGPD.

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 informazioni indicate dall'articolo 31 del RGPD.
2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema allegato B al presente disciplinare.
3. Il Responsabile del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.
4. Il formato del registro di cui al comma 2 può essere variato con atto del Segretario (Resp. Serv. AA.GG) per esigenze organizzative, fermo restando il contenuto minimo delle informazioni richieste dal RGPD.

Art.9 Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35 RGDP.
3. Nei casi di trattamenti riconducibili all'art. 35 del RGPD, il Titolare può escludere la necessità di effettuare la DPIA quando ritenga motivatamente che il trattamento non può presentare un rischio elevato. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.
4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Unione.
5. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

6. 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.

7. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

8. Il responsabile della sicurezza dei sistemi informativi, 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.

9. 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, p. 1, RGDP;
- 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.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

10. Per l'effettuazione della DPIA 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.

11. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

12. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 10 Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la

perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal 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 entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad 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 ad una violazione, in conformità al considerando 75 del RGPD, 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.
- decifrazione non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- 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 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. 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 in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art.11 Rinvio ed entrata in vigore

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.
2. La presente disciplina interna entra in vigore il giorno successivo all'inizio della pubblicazione della delibera di approvazione.

