



REGOLAMENTO PROTEZIONE DATI PERSONALI

Approvato con Deliberazione di Consiglio Provinciale n. 23 del 28/11/2019

SOMMARIO

GLOSSARIO	
Art. 1	Oggetto
Art. 2	Principi applicabili al trattamento e finalità del trattamento dei dati personali
Art. 3	Titolare del trattamento
Art. 4	Persone autorizzate al trattamento dei dati personali
Art. 5	Responsabili del trattamento
Art. 6	Responsabile della protezione dei dati (RPD)
Art. 7	Informativa
Art. 8	Comunicazione interna di documenti contenenti dati personali
Art. 9	Sicurezza del trattamento
Art. 10	Registro unico dei trattamenti
Art. 11	Valutazione d'impatto sulla protezione dei dati (DPIA)
Art. 12	Violazione dei dati personali
Art. 13	Rinvio

* GLOSSARIO *

Sulla base di quanto previsto dal Regolamento Europeo del 27 aprile 2016 n. 679 (*General Data Protection Regulation*), di seguito RGPD, ai fini del presente Regolamento si intende per:

1. «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2. «**dati particolari**»: i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i, dati biometrici, i dati relativi alla salute o all'orientamento sessuale della persona;
3. «**dati giudiziari**»: i dati personali relativi alle condanne penali e ai reati ed alle connesse misure di sicurezza;
4. «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie che forniscono informazioni univoche sulla fisiologia o sulla salute e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
5. «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali che consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
6. «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria in quanto rivelano informazioni relative al suo stato di salute;
7. «**interessato**»: la persona fisica titolare dei dati personali oggetto di trattamento;
8. «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione

mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

9. «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
10. «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
11. «**pseudonimizzazione**»: il trattamento dei dati personali eseguito in modo tale che i medesimi non possano essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire l'impossibilità ad associarli ad una persona fisica identificata o identificabile;
12. «**minimizzazione**»: evitare di usare dati personali non sono assolutamente indispensabili rispetto al trattamento da effettuare;
13. «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
14. «**persone autorizzate al trattamento dei dati personali**: ai fini del presente Regolamento provinciale per "persone autorizzate al trattamento di dati personali" si intendono:
 - persone autorizzate al trattamento dei dati personali con delega: corrispondono alle figure del Segretario Generale e dei Dirigenti dell'Ente e sono autorizzati al trattamento dei dati personali con delega del Presidente *pro tempore*, in qualità di Titolare del trattamento;
 - persone autorizzate al trattamento operative: i dipendenti dell'Ente autorizzati al trattamento dei dati in modo operativo con atto del Dirigente competente;
15. «**responsabili del trattamento**»: le persone fisiche o giuridiche, l'autorità pubblica, il servizio o altri organismi che trattano dati personali per conto del Titolare del trattamento;
16. «**incaricato del trattamento**»: chiunque, agendo sotto l'autorità del responsabile del trattamento o del titolare del trattamento, abbia accesso a dati personali essendo stato

autorizzato al loro trattamento;

17. «**responsabile della protezione dei dati**», RPD, il dipendente del titolare o del responsabile del trattamento ovvero la persona fisica o giuridica estranea all'organizzazione del Titolare o dei responsabili del trattamento che svolge le funzioni previste dall'art. 39 del RGPD o ulteriori compiti affidati dal titolare del trattamento sulla base di un contratto di servizi;
18. «**amministratore del sistema**»: la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché all'amministrazione di basi di dati, di reti e di apparati di sicurezza e di sistemi *software* complessi.
19. «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale viene manifestato l'assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento di dati personali che lo riguardano;
20. «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dall'Ente (*Data Breach*);
21. «**DPIA**»: Procedimento di valutazione di impatto sulla protezione dei dati.

REGOLAMENTO PROTEZIONE DATI PERSONALI

Art. 1 Oggetto

Il presente Regolamento disciplina le misure organizzative, procedurali e tecnologiche prescelte dall'Ente riguardo il trattamento dei dati di carattere personale concernenti le persone fisiche nonché la libera circolazione di tali dati.

Le norme ivi inserite sono adottate nel rispetto del Regolamento Europeo del 27 aprile 2016 n. 679 (*General Data Protection Regulation*), di seguito indicato con "RGPD", e dal D. Lgs. n. 196 del 30/06/2003 recante "*Codice in materia di protezione dei dati personali*", come modificato dal D. Lgs. del 10/08/2018 n. 101.

Le norme previste nel presente testo regolamentare sono definite ed applicate per garantire e dimostrare che il trattamento dei dati personali effettuato dalla Provincia di Fermo è conforme alla normativa vigente.

Art. 2 Principi applicabili al trattamento e finalità del trattamento dei dati personali

1. Precisato che la finalità del trattamento è tassativamente stabilita dalla fonte normativa che lo disciplina, i trattamenti dei dati personali sono compiuti dalla Provincia di Fermo per le seguenti finalità:

a) esercizio di una attività di interesse pubblico connessa allo svolgimento delle funzioni amministrative di competenza. In tale ambito rientra il trattamento di dati personali relativi a persone fisiche effettuato per lo svolgimento dei compiti istituzionali connessi all'esercizio delle funzioni fondamentali assegnate all'Ente dall'art. 1, commi 85, 86 ed 88, della L. 56 del 07/04/2014 "*Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni*", di seguito elencate in via generale:

- pianificazione territoriale provinciale di coordinamento, nonché tutela e valorizzazione dell'ambiente;
- pianificazione dei servizi di trasporto in ambito provinciale, autorizzazione e controllo in materia di trasporto privato, in coerenza con la programmazione regionale, nonché costruzione e gestione delle strade provinciali e regolazione della circolazione stradale ad esse inerente;
- programmazione provinciale della rete scolastica, nel rispetto della programmazione regionale;
- raccolta ed elaborazione di dati, assistenza tecnico-amministrativa agli Enti Locali;
- gestione dell'edilizia scolastica;
- controllo dei fenomeni discriminatori in ambito occupazionale e promozione delle pari opportunità sul territorio provinciale;

- adempimento di obblighi legali cui è soggetta la Provincia;
- esecuzione di contratto con soggetti interessati;
- predisposizione dei documenti di gara, di stazione appaltante (SUA), di monitoraggio dei contratti di servizio e di organizzazione di concorsi e procedure selettive;
- cura dello sviluppo strategico del territorio e gestione di servizi in forma associata in base alle specificità del territorio medesimo;

c) esercizio delle funzioni elettorali in sede di svolgimento delle elezioni provinciali di secondo grado per l'elezione degli organi provinciali nelle modalità stabilite dalla L. 56/2014;

d) specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

2. In attuazione ai principi generali di cui all'art. 5 del RGPD, nell'esercizio delle funzioni politiche ed amministrative declinate al comma precedente, l'Ente tratta i dati personali:

- in modo lecito, corretto e trasparente;
- per finalità determinate, esplicite e legittime e, se utilizzati e conservati nel corso del tempo, in modo compatibile con le finalità iniziali;
- in modo adeguato, pertinente e limitato alle effettive finalità;
- in modo esatto, aggiornando i dati se necessario;
- consentendo l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati sono trattati.

Art. 3

Titolare del trattamento

1. La Provincia di Fermo (di seguito Titolare), rappresentata ai fini previsti dal DGPR dal Presidente *pro tempore*, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee, utilizzate dai Settori dell'Ente nell'espletamento dell'attività amministrativa.
2. Il Titolare mette in atto le misure tecniche ed organizzative adeguate a garantire e dimostrare il rispetto dei principi generali stabiliti dall'art. 5 del RGPD, riportati all'art. 2, comma 2, del presente Regolamento. A tal fine adotta, dalla fase della progettazione, avvio e conclusione dei procedimenti, le procedure organizzative adeguate a garantire e dimostrare che il trattamento dei dati è conforme ai principi della legislazione comunitaria.
3. Il Titolare illustra annualmente, nell'ambito della programmazione operativa del bilancio annuale di previsione, in particolare nel documento unico di programmazione (DUP), le misure tecniche ed organizzative adottate, se necessario aggiornate, atte a garantire la conformità al RGPD, tenuto conto dei costi di attuazione, della natura dei dati, dell'ambito di applicazione, del

contesto, delle finalità del trattamento, della struttura dell'Ente e, non da ultimo, dei rischi connessi al trattamento.

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

- le informazioni indicate dall'art. 13 del RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
- le informazioni indicate dall'art. 14 del RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato;
- le agevolazioni necessarie all'esercizio dei diritti dell'interessato stabiliti dagli artt. 15-22 del RGPD.

5. Sulla *home page* del sito istituzionale dell'Ente, corrispondente all'indirizzo www.provincia.fm.it, è consultabile e ininterrottamente aggiornata la pagina *web* denominata "RGPD - PRIVACY", dedicata alla consultazione delle informative e degli indirizzi adottati dall'Amministrazione in materia di politiche di protezione dei dati personali. Da tale pagina è possibile conoscere l'organigramma della privacy vigente, le informative privacy complete nonché comunicare con il Responsabile della Protezione dati (RPD) di cui all'art. 6 del presente Regolamento attraverso l'indirizzo di posta elettronica "rp@provincia.fm.it".

6. Il Titolare del trattamento provvede inoltre a:

- nominare il Responsabile della Protezione dei Dati (RPD);
- delegare il Segretario Generale ed i Dirigenti al trattamento di dati personali;
- nominare l'Amministratore del sistema informatico;
- diramare le direttive interne necessarie per l'applicazione delle disposizioni del RGPD e del presente Regolamento, sentiti il RPD, il Segretario Generale, i Dirigenti, i responsabili del trattamento e l'amministrazione del sistema informatico.

7. Nel caso in cui un tipo di trattamento, specie nel caso di uso delle nuove tecnologie, presenti un rischio elevato per i diritti e le libertà delle persone fisiche, spetta al Titolare effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 del RGPD, sulla base di quanto dettagliato all'art. 8 del presente Regolamento, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento medesimo.

8. Nel caso in cui due o più Titolari del trattamento determinano congiuntamente le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del RGPD. Mediante accordo vengono definite le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di applicazione del RGPD, 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.

Art. 4

Persone autorizzate al trattamento dei dati personali

1. Nell'espletamento dei propri compiti istituzionali, la Provincia si avvale obbligatoriamente di uno più persone autorizzate al trattamento di dati personali. Nell'ambito della struttura organizzativa dell'Ente, le persone autorizzate al trattamento si distinguono in:
 - persone autorizzate al trattamento dei dati personali con delega: corrispondono alle figure del Segretario Generale e dei Dirigenti, autorizzati al trattamento dei dati personali con delega del Presidente *pro tempore*, in qualità di Titolare del trattamento;
 - persone autorizzate al trattamento operative: i dipendenti dell'Ente autorizzati al trattamento dei dati in modo operativo con atto del Dirigente competente.
2. L'autorizzazione al trattamento dei dati personali nei riguardi del Segretario Generale e dei Dirigenti può avvenire contestualmente al decreto di attribuzione delle funzioni dirigenziali oppure con separato decreto.
3. I soggetti autorizzati al trattamento dati ai sensi del comma 1 devono offrire garanzie in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, nonché adottare le misure tecniche e organizzative individuate all'art. 9 del presente Regolamento, atte a garantire che il trattamento sia effettuato in conformità al RGPD. Essi assicurano altresì che chiunque agisca sotto la propria autorità ed abbia accesso a dati personali nell'ambito dell'articolazione organizzativa di competenza, possieda apposita formazione ed istruzione ed osservi un adeguato obbligo legale di riservatezza.
4. Nell'ambito delle risorse umane assegnate al Settore di competenza, il Segretario Generale ed i Dirigenti autorizzati al trattamento, possono individuare con proprio atto i dipendenti autorizzati al trattamento dei dati in modo operativo. Le operazioni di trattamento possono infatti essere effettuate solo da incaricati, autorizzati al trattamento, che operano sotto la diretta autorità del Dirigente preposto, attenendosi alle istruzioni impartite per iscritto e previa individuazione dell'ambito di trattamento consentito.
Il Dirigente risponde, anche dinanzi al Titolare, dell'operato dei dipendenti operativi autorizzati al trattamento, 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 di aver vigilato in modo adeguato sull'operato dei dipendenti autorizzati.
5. Il Segretario Generale ed i Dirigenti autorizzati al trattamento dei dati osservano la normativa richiamata in via generale all'art. 1 del presente Regolamento e sovrintendono ai compiti ed alle istruzioni affidategli dal Titolare, analiticamente specificate per iscritto nell'atto di autorizzazione. In via generale, provvedono:
 - all'adozione di idonee misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti sulla base di quanto successivamente previsto all'art. 9 del presente Regolamento;

- alla tenuta del registro unico dei trattamenti di cui all’art. 10 del presente Regolamento;
- alla sensibilizzazione e formazione del personale assegnato 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 (DPIA) fornendo adeguato supporto tecnico e giuridico;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. “*data breach*”) ai fini della successiva notifica della violazione al Garante, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

6. Il Segretario Generale ed i Dirigenti autorizzati al trattamento di dati personali conservano, presso la propria struttura organizzativa e in formato elettronico, un registro delle categorie di attività relative al trattamento svolte per conto del Titolare in cui sono indicate le seguenti informazioni:

- il nome ed i dati di contatto dei dipendenti che, nell’ambito del proprio Settore e ai sensi del comma 4 del presente articolo, sono stati autorizzati con proprio atto al trattamento dei dati personali;
- le categorie di trattamenti effettuati per conto del Titolare;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

7. Il Segretario Generale e i Dirigenti autorizzati al trattamento mettono a disposizione del Titolare la documentazione atta a dimostrare il rispetto degli obblighi nonché consentire la realizzazione di revisioni, comprese le ispezioni, da parte del Titolare del trattamento o di un altro revisore che lui ha incaricato, e contribuire a queste revisioni.

Art. 5 **Responsabili del trattamento**

Il Segretario Generale ed i Dirigenti autorizzati al trattamento possono avvalersi, al fine del compimento delle funzioni amministrative di competenza, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui all’art. 2 del presente Regolamento.

A tal fine nelle convenzioni, nelle concessioni, nei contratti, negli incarichi professionali o negli altri strumenti giuridici consentiti dalla legge con cui è affidata a soggetti esterni alla Provincia la gestione di attività e/o servizi che prevedono il trattamento di dati personali, è prevista la nomina di Responsabile del trattamento dei dati personali in relazione alle attività affidate. Gli atti di affidamento specificano la finalità perseguita, la tipologia di dati trattati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità del trattamento.

Qualora, negli atti vigenti o da adottare, manchi tale previsione, sarà cura dei del Segretario Generale e dei Dirigenti effettuare l’adeguamento degli strumenti contrattuali sottoscritti.

Art. 6
Responsabile della protezione dei dati (RPD)

1. Il Responsabile della protezione dei dati (in seguito indicato con “RPD”) può essere nominato tra i dipendenti di ruolo della Provincia, di qualifica non inferiore alla cat. D, purché in possesso delle qualità professionali previste dall’art. 37 del RGPD, in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati e della capacità di assolvere ai compiti di cui all’art. 39 del RGPD.
2. Nel caso in cui tra i dipendenti della Provincia non sia possibile individuare il RPD, l’incarico può essere affidato ad un soggetto esterno all’Amministrazione in possesso di comprovata e approfondita conoscenza della materia e della struttura organizzativa dell’Ente.
3. In tal caso i compiti attribuiti al RPD, indicati in apposito contratto di servizio, sono i seguenti:
 - informare e fornire consulenza al Titolare del trattamento, al Segretario Generale ed ai Dirigenti autorizzati al trattamento, ai Responsabili del trattamento nonché a tutto il personale operativo autorizzato ex art. 4, comma 4, riguardo gli obblighi derivanti dal RGPD e, in generale, dalla normativa in materia di protezione dei dati richiamata all’art. 1, vigilando sulla sua effettiva e corretta applicazione, incluso il presente Regolamento provinciale;
 - fornire, se richiesto, un parere in merito alla valutazione d’impatto sulla protezione dei dati (DPIA) e collaborare allo svolgimento della medesima;
 - cooperare con il Garante fungendo da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all’art. 36 del RGPD ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare del trattamento al Garante;
 - tenuta, in forma telematica, del registro unico dei trattamenti di cui all’art. 10 del presente Regolamento;
 - svolgere gli altri compiti e funzioni a condizione che il Titolare, il Segretario Generale, i Dirigenti autorizzati al trattamento ed i responsabili del trattamento verifichino previamente la insussistenza di conflitto di interessi.
4. La figura del RPD 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 Segretario generale ed i Dirigenti autorizzati al trattamento con delega;
 - i Responsabili del trattamento di cui all’art. 5 del presente Regolamento;
 - qualunque incarico che comporta la funzione di determinazione delle finalità e mezzi del trattamento.

5. È possibile l'affidamento dell'incarico di RPD ad un unico soggetto, anche esterno, designato da più Comuni mediante esercizio associato della funzione nelle forme previste dal D. Lgs. 18 agosto 2000 n. 267.
6. Il Titolare o il Segretario Generale e i Dirigenti autorizzati al trattamento dei dati personali assicurano che il RPD sia tempestivamente e adeguatamente coinvolto nei procedimenti che possono incidere su questioni attinenti alla protezione dei dati personali. A tal fine il RPD:
- può partecipare alle riunioni di coordinamento delle figure apicali che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
 - deve essere in possesso delle informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea al riguardo;
 - esprime un parere, obbligatorio ma non vincolante, sulle decisioni che impattano sulla protezione dei dati e, nel caso in cui la decisione assunta dal Titolare o dai Dirigenti autorizzati al trattamento con delega determini una condotta difforme da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
 - deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente (*Data Breach*) al fine di procedere alla segnalazione all'Autorità;
 - svolge con cadenza almeno semestrale incontri presso la sede dell'Ente redigendo apposito verbale.
7. Nello svolgimento dei compiti affidatigli, il RPD deve preliminarmente esaminare i rischi potenziali ed effettivi inerenti al trattamento dei dati personali, avuto riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del medesimo. A tal fine il RPD:
- effettua la mappatura delle aree di attività, valutandone il grado di rischio in termini di protezione dei dati;
 - definisce un ordine di priorità nell'attività da svolgere incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati.
8. Il RPD opera in posizione di autonomia nello svolgimento dei compiti attribuiti riferendo direttamente al Titolare ed ai Responsabili del trattamento. Nel caso in cui siano rilevate dal RPD o comunque sottoposte alla sua attenzione, decisioni incompatibili con il RGPD e con le indicazioni da egli stesso fornite, è tenuto a manifestare il proprio dissenso comunicandolo al Titolare ed ai Dirigenti autorizzati al trattamento con delega.

Art.7 **Informativa**

1. La Provincia di Fermo, in qualità di Titolare del trattamento, predispone l'informativa generale sul trattamento dei dati personali onde fornire all'interessato tutte le informazioni relative al trattamento dei dati in forma concisa, trasparente e facilmente intellegibile.

Le informazioni da rendere ai sensi dell'art. 13 del RGPD, riportano quanto segue:

- generalità e contatti del Titolare del trattamento e del RPD;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari di dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione al trattamento, oltre al diritto alla portabilità dei dati;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo ad una Autorità di controllo;
- se la comunicazione dei dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

2. L'informativa di cui al comma precedente viene resa agli interessati attraverso la pubblicazione e l'aggiornamento di apposito documento sulla pagina *web* indicata all'art. 3, comma 5, del presente Regolamento e, qualora ritenuto opportuno, viene resa in forma sintetica all'avvio del procedimento amministrativo posto in essere.

Art.8

Comunicazione interna di documenti contenenti dati personali

La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lett. a) del DPR n. 445/2000, contenenti dati personali ai componenti degli organi di governo, ovvero all'interno della struttura organizzativa di questa Provincia, per ragioni d'ufficio e nell'ambito delle specifiche competenze dei servizi, non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti.

Il Segretario Generale ed i Dirigenti autorizzati al trattamento con delega possono tuttavia disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione coinvolga dati particolari e/o giudiziari.

Art. 9

Sicurezza del trattamento

1. La Provincia di Fermo adotta le misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, elencate in modo non tassativo al comma 2 del presente articolo, tenendo conto dello stato dell'arte, 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 adottate dalla Provincia di Fermo per ridurre i rischi del trattamento ricomprendono, in via generale:
 - la pseudominimizzazione: conservazione e pubblicazione dei dati in una forma che impedisca l'identificazione del soggetto interessato senza l'utilizzo di informazioni aggiuntive, conservate separatamente e soggette a misure tecniche e organizzative che garantiscano la non attribuibilità ad una persona fisica identificata o identificabile;
 - la minimizzazione: utilizzo dei soli dati personali assolutamente indispensabili rispetto al trattamento da effettuare;
 - la cifratura: se il trattamento prevede la gestione di dati ultrasensibili, il Segretario Generale o il competente Dirigente valuta l'opportunità di innalzare il livello di sicurezza attraverso l'adozione della tecnica di crittografia, vale a dire il processo volto a impedire la leggibilità in chiaro di un testo a chi non abbia il sistema di cifratura e la chiave per decifrare il testo stesso, anch'esso conservato separatamente;
 - la capacità di assicurare la continua riservatezza, l'integrità, la disponibilità e la 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;
 - possibilità di verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento.

3. Costituiscono ulteriori misure tecniche ed organizzative che possono essere adottate dall'Ente:
 - l'utilizzo di sistemi di autenticazione;
 - l'utilizzo di sistemi di autorizzazione;
 - l'utilizzo e l'aggiornamento di sistemi di protezione delle banche dati telematiche (antivirus, firewall, antintrusione, altro);
 - la predisposizione di idonee misure antincendio;
 - l'utilizzo di sistemi di rilevazione di intrusione, di sorveglianza e l'eventuale registrazione degli accessi;
 - la presenza di porte, armadi e contenitori dotati di serrature e costruite in materiale ignifugo;
 - la presenza di sistemi di copiatura e conservazione di archivi elettronici;
 - l'adozione di misure che consentono il ripristino tempestivo della disponibilità e dell'accesso dei dati in caso di incidente fisico o tecnico;
 - l'applicazione di ogni ulteriore misura ritenuta utile.

4. La conformità delle applicazioni delle misure di sicurezza sopra elencate 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.

5. Il Titolare, il Segretario Generale ed i Dirigenti autorizzati al trattamento nonché l'Amministratore del sistema informatico e il RPD provvedono, per quanto di rispettiva competenza, a impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

Art. 10

Registro unico dei trattamenti

1. Il Registro delle attività di trattamento svolte dall'Ente in qualità di Titolare del trattamento reca le seguenti informazioni di base:
 - il nome ed i dati di contatto del Titolare del trattamento, del Segretario Generale e dei Dirigenti autorizzati al trattamento con delega e del RPD;
 - le categorie di trattamenti effettuate dal Segretario Generale e dai Dirigenti autorizzati al trattamento in relazione alla raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, consultazione, uso, comunicazione, pseudonomizzazione ed ogni altra operazione applicata a dati personali;
 - il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, ed elencate al precedente art. 7 del presente Regolamento;
 - le finalità del trattamento;
 - la sintetica descrizione delle categorie di soggetti interessati, nonché le categorie di dati personali;
 - le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
 - ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati.
1. Il Registro è tenuto dal Titolare in forma telematica, anche attraverso specifici applicativi telematici, può contenere informazioni accessorie tenuto conto della struttura organizzativa e tecnologica dell'Ente.
2. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro unico dei trattamenti, sotto la responsabilità del Segretario Generale e dei Dirigenti autorizzati al trattamento.

Art. 11

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 infatti attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 del RGPD, considerando la natura, l'oggetto,

il contesto, le finalità dello stesso trattamento, la effettiva necessità oltre che facilitare la gestione del rischio per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali e permette di realizzare e dimostrare la conformità del trattamento ai principi del RGPD.

2. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa, pur potendo materialmente affidarne la conduzione ad altro soggetto interno o esterno alla Provincia, previa consultazione con il RPD, anche per assumere la decisione di effettuare o meno la DPIA. La consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA e monitorate dal RPD.
3. Si ritiene non necessaria la DPIA nei casi seguenti:
 - quando il trattamento non comporta un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, comma 1, del RGPD.;
 - 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;
 - 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 e sia già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
4. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
 - a. descrizione sistematica del contesto, dei trattamenti previsti, delle finalità trattamento, tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
 - b. valutazione della necessità e proporzionalità dei trattamenti, sulla base:
 - delle finalità specifiche, esplicite e legittime;
 - della liceità del trattamento;
 - dei dati adeguati, pertinenti e limitati a quanto necessario;
 - del periodo limitato di conservazione;
 - delle informazioni fornite agli interessati;
 - del diritto di accesso e portabilità dei dati;
 - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
 - dei rapporti con i responsabili del trattamento;
 - delle garanzie per i trasferimenti internazionali di dati;
 - consultazione preventiva del Garante privacy;

- c. valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
- d. individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

5. 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.

6. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA eseguita indica 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.

7. 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. 12

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 dalla Provincia.

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 Segretario Generale ed i Dirigenti sono obbligati ad informare il Titolare, senza ritardo, tutti i casi di possibile violazione del trattamento di dati.

3. 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.

4. La notifica deve avere il contenuto minimo previsto dall'art. 33 del RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

5. 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.13

Rinvio

Per tutto quanto non espressamente disciplinato con le presenti norme, si applicano le disposizioni del Regolamento Europeo del 27 aprile 2016 n. 679 (*General Data Protection Regulation*) e del D. Lgs. adottato il 30/06/2003 n. 196 recante "*Codice in materia di protezione dei dati personali*", come modificato dal D. Lgs. del 10/08/2018 n. 101 e comunque tutte le sue norme attuative vigenti.