

PROVINCIA DI ORISTANO

PROVÌNTZIA DE ARISTANIS

***Regolamento di attuazione del Regolamento UE 2016/679
relativo alla protezione delle persone fisiche con riguardo
al trattamento dei dati personali.***

SOMMARIO

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. 8	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

Allegati

- A) Schema di registro attività di trattamento
- B) Schema di registro categorie attività di trattamento
- C) Schema di registro unico dei trattamenti
- D) Glossario Regolamento
- E) Glossario Registri

Articolo 1

Oggetto

1. Il presente Regolamento ha per oggetto misure procedurali 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, nella Provincia di Oristano).

Articolo 2

Titolare del trattamento

1. La Provincia di Oristano nella persona del legale rappresentante pro-tempore, è il Titolare del trattamento dei dati personali raccolti o meno 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 all'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 e dimostrare, che il trattamento dei dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla base della 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. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di PEG, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento, come anche dei rischi dallo stesso derivati.
4. 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 sono stati ottenuti presso lo stesso interessato;
 - c) nel caso in cui un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare effettua una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata come "DPIA") ai sensi dell'art. 35 RGPD, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.
5. Il Titolare, inoltre, provvede a:
 - a) designare i Responsabili del trattamento nelle persone dei Dirigenti e dei Funzionari delle singole strutture in cui si articola l'organizzazione della Provincia che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative

di loro competenza; per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

- b) nominare il Responsabile della protezione dei dati (in seguito indicato con "DPO", acronimo di Data Protection Officer);
- c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto della Provincia, relativamente alle banche dati gestite da soggetti esterni alla Provincia, 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;
- d) predisporre l'elenco di Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

Articolo 3

Finalità del trattamento

1. I trattamenti sono compiuti dalla Provincia con le seguenti finalità:
 - a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e alle funzioni di competenza affidate dalla 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 la Provincia; la finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
 - c) l'esecuzione di un contratto con soggetti interessati;
 - d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento;

Articolo 4

Responsabile del trattamento

1. I Dirigenti sono nominati Responsabili del trattamento delle banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile, previa adeguata formazione, metterà in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD;
2. La designazione dei Responsabili del trattamento, di norma è contenuta nel decreto di incarico dirigenziale, con riferimento alla materia trattata, alla durata, alla natura, alle finalità del trattamento o dei trattamenti assegnati alla articolazione organizzativa assegnata;
3. Il Titolare può avvalersi, per il trattamento dei dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, 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.

4. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione di dati personali oppure dalla Commissione europea.
5. E' consentita la nomina da parte dei Dirigenti di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; gli incaricati operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto, che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile dovrà adeguatamente vigilare sull'operato del sub-responsabile.
6. il Titolare garantirà che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia impegnato alla riservatezza o abbia un adeguato obbligo legale di riservatezza e assicurerà a tali soggetti adeguata formazione.
7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza:
 - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare, salvo i casi di individuazione di altro soggetto;
 - all'adozione di 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 (DPO), se a ciò domandato 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 della Privacy qualora sia probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Articolo 5

Responsabile della protezione dati

1. Il Responsabile della protezione dei dati è individuato nella figura unica di un dipendente di ruolo della Provincia di qualifica non inferiore alla Cat. D in altro soggetto esterno, scelto tramite procedure di legge. L'DPO dovrà essere in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica delle normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno e mantenendo la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

Il DPO è incaricato dei seguenti compiti:

- a) informare e fornire consulenza al Titolare e al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal RGPD 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 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 DPO in merito a:
 1. se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA;
 2. se condurre la DPIA con le risorse interne ovvero esternalizzandola;
 3. quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
 4. se la DPIA sia stata condotta correttamente o meno;
 5. 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 ad ogni altra questione. A tali fini il nominativo del DPO 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, su delega del Titolare;
 - 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, al fine di salvaguardare gli obblighi di indipendenza del DPO.
1. 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 dirigenti e dei Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;
 - il DPO deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una idonea consulenza;
 - il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante; nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificatamente tale decisione;
 - il DPO deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

1. 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 — ovvero 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.

2. 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.

3. La figura di DPO è incompatibile con chi determina le finalità o i mezzi dei trattamento; in particolare, risultano con la stessa incompatibili:
 - il Responsabile per la prevenzione della corruzione e per la trasparenza;
 - il Responsabile del trattamento;
 - il Responsabile del servizio informatico;
 - qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento, compatibilmente con l'assetto organizzativo della Provincia.

1. Il Titolare ed il Responsabile del trattamento assicurano al DPO:
 - la comunicazione ufficiale della nomina a tutto il personale in modo da garantire che la sua presenza e le sue funzioni siano nota all'interno dell'Ente;
 - il supporto, le informazioni e gli input essenziali da parte dei Settori dell'Ente.

1. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

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

Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare od al Responsabile del trattamento.

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

Articolo 6

Sicurezza del trattamento¹

2. La Provincia di Oristano 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.
3. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione (ovvero il principio per cui le informazioni di profilazione debbano essere conservate in una forma che impedisce l'identificazione dell'utente. Due metodi tipici sono il mascheramento e l'utilizzo dei tag), la minimizzazione, che impone che i dati personali debbano sempre essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, co. 1, lett. c, GDPR); 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.
4. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Settore 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.
1. 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.
2. La Provincia 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.
3. 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 della Provincia, Sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

¹ l'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettata) sia all'atto del trattamento.

4. 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).

Articolo 7

Registro delle attività di trattamento

5. Il Registro delle attività di trattamento svolte dal titolare del trattamento reca almeno le seguenti informazioni:
 - a) il nome ed i dati di contatto della Provincia, del legale rappresentante, del suo delegato ai sensi del precedente art. 2, del DPO;
 - b) le finalità di trattamento;
 - c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
 - d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
 - e) l'eventuale trasferimento di dati personali verso un paese terzo o 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.
6. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa della Provincia in forma telematica/cartacea, secondo lo schema allegato A al presente Regolamento; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.
7. Il Titolare del trattamento può decidere di affidare al DPO il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.
8. Il Titolare può stabilire 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, secondo lo schema allegato C al presente Regolamento. In tal caso, il Titolare delega la sua tenuta al Responsabile del trattamento di cui al precedente art. 4 o, comunque, ad un solo Responsabile dei trattamenti, ovvero può decidere di affidare tale compito al DPO, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Articolo 8

Registro delle categorie di attività trattate

9. Il Registro delle categorie di attività trattate da ciascun Responsabile di cui al precedente art. 4, reca le seguenti informazioni:
 - a) il nome ed i dati di contatto del Responsabile del trattamento e del DPO;

- b) le categorie di trattamenti effettuati da ciascun Responsabile. 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.
10. 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 regolamento.
11. Il Responsabile del trattamento può decidere di affidare al DPO il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

Articolo 9

Valutazioni d'impatto sulla protezione dei dati

12. 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.
13. 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, pp. 4-6, RGDP.
14. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p.3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono 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) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;

- e) trattamenti di dati su larga scala, tenendo conto: 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 ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

15. 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 alla Provincia.

Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il Responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento 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.

16. 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.

17. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà delle 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 DPO 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.

1. 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 e tendo 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) la 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;
 - a) 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;
 - b) 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 degli interessi legittimi degli interessati e delle altre persone in questione.
2. 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.
3. 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 i trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
4. 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.

Articolo 10

Violazione dei dati personali

5. 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.

6. 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, dopo essere venuto a conoscenza della violazione.

7. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, cin 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;
 - decifratura non autorizzata della pseudonimizzazione;
 - pregiudizio alla reputazione;
 - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari);

1. 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 e i dati personali verificatisi. 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).

1. 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.

2. 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.

Articolo 11

Rinvio

3. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

D) GLOSSARIO REGOLAMENTO

Ai fini del Regolamento, si intende per:

◆ **Titolare del trattamento**

l'autorità pubblica (la Provincia o altro ente locale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.

◆ **Responsabile del trattamento**

il Dirigente che tratta dati personali per conto del Titolare del trattamento.

◆ **Sub Responsabile del trattamento**

il dipendente della struttura organizzativa della Provincia, incaricato dal Responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento (elabora o utilizza materialmente i dati personali).

◆ **Responsabile per la protezione dei dati (Data Protection Officer)— DPO**

il dipendente della struttura organizzativa della Provincia, il professionista privato o impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento, figura di alto livello professionale, deve essere prontamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e godere di ampia autonomia.

◆ **Registri delle attività di trattamento**

elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze.

◆ **DPIA — "Data Protection Impact Assessment" — Valutazione d'impatto sulla protezione dei dati**

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

◆ **Garante Privacy**

il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n° 765, quale autorità amministrativa pubblica di controllo indipendente.

E) GLOSSARIO REGISTRI

Ai fini delle proposte dei registri, si intende per:

◆ **Categorie di trattamento**

Raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

◆ **Categorie di dati personali**

- Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale.
- Dati inerenti lo stile di vita: situazione economica, finanziaria, patrimoniale, fiscale.
- Dati connessione: indirizzo IP, login, altro.
- Dati di localizzazione: ubicazione, GPS, GSM, altro.

◆ **Finalità del trattamento**

- Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico; la gestione dei servizi di statistica; l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate alla Provincia
- Adempimento di un obbligo legale al quale è soggetto la Provincia
- Esecuzione di un contratto con i soggetti interessati
- Altre specifiche e diverse finalità.

◆ **Misure tecniche ed organizzative**

- Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.
- Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro), adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.
- Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

◆ **Dati sensibili**

Dati inerenti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita o l'orientamento sessuale, dati genetici o biometrici, dati relativi a condanne penali.

◆ **Categorie interessati**

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

◆ **Categorie destinatari**

Persone fisiche; autorità pubbliche ed altre P.A. ; persone giuridiche private; altri soggetti.