I REGOLAMENTI PROVINCIALI:
N.93

PROVINCIA DI PADOVA

REGOLAMENTO SUL TRATTAMENTO DEI DATI PERSONALI

Approvato con D.C.P. in data 24.9.2020 n. 14

PROVINCIA DI PADOVA

REGOLAMENTO

SUL TRATTAMENTO DEI DATI PERSONALI

Indice generale

CAPO I – DISPOSIZIONI GENERALI

Art. 1 – Oggetto del regolamento

1. Il presente regolamento disciplina le modalità, le procedure e le misure per il trattamento dei dati personali contenuti nelle banche dati ed archivi gestiti e utilizzati dalla Provincia, in forma informatizzata e non, in attuazione del Regolamento europeo n. 679 del 27 aprile 2016 e della disciplina nazionale.
2. Per quanto non previsto nel presente regolamento si rinvia al predetto Regolamento europeo 2016/679, alle vigenti fonti di diritto europee e nazionali, alle linee guida e ai provvedimenti del Garante della Privacy, alle direttive impartite dal Titolare del trattamento, dall'Amministratore del sistema informatico e dal Responsabile della protezione dei dati.

Art. 2 – Definizioni

1. Ai fini del presente regolamento, si intende per :
   a) "**Provincia**": la Provincia di Padova;
   b) "**Titolare**": la Provincia di Padova nella qualità di titolare del trattamento dei dati personali;
   c) "**Responsabili esterni**": i soggetti esterni, incaricati o appaltatori o concessionari, che assumono gli obblighi previsti dal Regolamento e dal Codice;
   d) "**Sub-responsabili**": i soggetti nominati come tali dal "responsabile" a seguito autorizzazione del Titolare;
   e) **"Amministratore di sistema**" si intendono, in ambito informatico, le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente regolamento vengono sono equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi s*oftware* complessi;
   f) "**RPD**": il Responsabile della Protezione Dati;
   g) "**Garante**": il Garante per la protezione dei dati personali;
   h) "**Codice**": il decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;
   i) "**Regolamento**" o "RGPD": il Regolamento europeo del 27 aprile 2016 n. 679 (General Data Protection Regulation);
   j) "**Autorizzati**": i dipendenti della Provincia incaricati del trattamento di dati e di accedere e gestire banche dati dell'ente;
   k) «**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;

l) "**Categorie particolari di dati personali**" : i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

m) **Dati giudiziari**»: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

n) «**Dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

o) «**Dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

p) «**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, che rivelano informazioni relative al suo stato di salute;

q) «**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;

r) «**Interessato**»: la persona fisica titolare dei dati personali oggetto di trattamento;

s) "**Valutazione dell'impatto del trattamento**" o "DPIA": la valutazione dell'impatto del trattamento sulla protezione dei dati personali ai sensi dell'art. 35, RGDP;

t) "**Data breach**": la violazione dei dati personali.

2. Si richiamano, in quanto vigenti le altre definizioni di cui all'art. 4 del Regolamento UE 2016/679.

Art. 3 – Finalità del trattamento

1. La Provincia provvede al trattamento dei dati personali soltanto per lo svolgimento delle proprie funzioni istituzionali, nei limiti stabiliti dalle disposizioni normative europee, nazionali e provinciali.
2. In particolare, i trattamenti sono compiuti per le seguenti finalità generali:

- esecuzione di attività di interesse pubblico o connesse all'esercizio di pubblici poteri, come corrispondenti alle funzioni proprie o esercitate dalla Provincia, anche in materia di servizi pubblici, formativi, informativi, assetto ed utilizzazione del territorio;
- l'adempimento di un obbligo legale al quale è soggetta la Provincia, anche in connessione ai procedimenti, ivi compresi quelli sanzionatori, che gestisce;
- l'esecuzione di un contratto (anche di lavoro subordinato) o un accordo con soggetti interessati;
- per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

3. La finalità del trattamento è connessa alla fonte normativa che lo disciplina. Nel *registro delle attività di trattamento* sono indicate le finalità particolari sottese ai trattamenti.

Art. 4 – Modalità di trattamento

1. I dati personali sono trattati dalla Provincia con modalità atte ad assicurare il rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato, secondo quanto dettagliato nel *registro delle attività di trattamento* e nella documentazione attuativa del presente regolamento.

Art. 5 – Trattamento in violazione

1. I dati personali trattati in violazione della relativa disciplina non possono essere utilizzati.

Art. 6 – Consenso dell'interessato

1. Questa Provincia non deve richiedere agli interessati il consenso per il trattamento dei loro dati personali allorquando il trattamento dei dati è effettuato nello svolgimento dei propri compiti istituzionali di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito dal diritto dell'Unione o dello Stato.
2. Nelle fattispecie diverse da quelle di cui al precedente comma 1, qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
3. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

CAPO II – TRATTAMENTO DI PARTICOLARI CATEGORIE DI DATI

Art. 7 – Dati sensibili

1. È vietato trattare i dati personali di cui all'art. 9, paragrafo 1, del "Regolamento", che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2. I trattamenti delle predette categorie di dati personali, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del precitato articolo del "Regolamento", sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonche' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
3. Si considerano di rilevante interesse pubblico i trattamenti afferenti le materie indicate nell'art. 2-*sexies*, del D.Lgs. 196/2003 e s.m.i.
4. Il divieto del trattamento dei dati particolari di cui al presente articolo non si applica se si verifica uno dei casi indicati nell'art. 9, paragrafo 2, del "Regolamento".

Art. 8 – Dati relativi a condanne penali e reati

1. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, sulla base delle condizioni di liceità del trattamento di cui all'art. 6, paragrafo 1, del "Regolamento", deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dello Stato che preveda garanzie appropriate per i diritti e le libertà degli interessati.
2. Fatto salvo quanto previsto dal D.Lgs. n. 51/2018, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del "Regolamento", che non avviene sotto il controllo dell'autorita' pubblica, e' consentito, ai sensi dell'articolo 10 del medesimo "Regolamento", solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le liberta' degli interessati. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui trattasi nonche' le relative garanzie sono individuati con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante.
3. Fermo restando quanto indicato nel comma precedente, il trattamento dei dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti le materie indicate nell'art. 2-oct*ies*, comma 3, del D.Lgs. 196/2003 e s.m.i.

CAPO III – DIRITTI DELL'INTERESSATO

Art. 9 – Informativa raccolta dati presso l'interessato

1. La Provincia, nei casi di cui al precedente art. 6, comma 1, di raccolta di dati personali presso l'interessato, deve rendere allo stesso l'informativa sulla protezione dei dati personali, recante le indicazioni di cui all'art. 13 del GDPR.
2. Il Servizio Affari Generali redige ed aggiorna una informativa standard valevole per tutto l'Ente, da completarsi da parte dei dirigenti a seconda delle finalità dei rispettivi procedimenti.
3. L'informativa deve essere allegata a qualsiasi tipologia di procedimento per il quale si rende necessaria una raccolta di dati personali presso l'interessato ed allegata alla modulistica presente nel sito web istituzionale.

Art. 10 – Diritto di accesso

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, ottenere l'accesso ai dati personali, alle informazioni e con i limiti indicati nell'art. 15 del "Regolamento".
2. L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
3. L'interessato, con la richiesta di accesso, deve dimostrare la propria identità, inoltrando domanda corredata da documento di identità in corso di validità, anche via mail o mediante richiesta sottoscritta con firma digitale o equivalente trasmessa via PEC.
4. Le informazioni sono fornite per iscritto con le metodologie e tecniche dell'informatica e delle telecomunicazioni o, se necessario, mediante risposta cartacea. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata l'identità dell'interessato.

Art. 11 – Diritto di rettifica e integrazione

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano o l'integrazione dei dati personali incompleti, ai sensi dell'art. 16 del "Regolamento".
2. L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
3. L'interessato deve dimostrare la propria identità, inoltrando domanda corredata da documento di identità in corso di validità, anche via mail o mediante richiesta sottoscritta con firma digitale o equivalente trasmessa via PEC.
4. Alla rettifica ovvero all'integrazione dei dati richiesta dall'interessato provvede, senza ritardo e comunque entro cinque giorni lavorativi dalla data di arrivo della predetta istanza, il Responsabile del procedimento amministrativo cui ineriscono i dati da rettificare o integrare.

5. Dell'eseguita rettifica o integrazione ovvero della motivata inammissibilità è data tempestiva comunicazione all'interessato con raccomandata con avviso di ricevimento o con notifica a mani o tramite PEC.
6. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Art. 12 – Diritto di cancellazione (diritto all'oblio)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, qualora sussista uno dei motivi indicati nell'art. 17 del "Regolamento", con i limiti e le esclusioni ivi stabilite.
2. L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
3. L'interessato deve dimostrare la propria identità, inoltrando domanda corredata da documento di identità in corso di validità, anche via mail o mediante richiesta sottoscritta con firma digitale o equivalente trasmessa via PEC.
4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali, la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Art. 13 – Diritto di limitazione

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione dei dati personali che lo riguardano nelle ipotesi stabilite dall'art. 18 del "Regolamento".
2. L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
3. L'interessato deve dimostrare la propria identità, inoltrando domanda corredata da documento di identità in corso di validità, anche via mail o mediante richiesta sottoscritta con firma digitale o equivalente trasmessa via PEC.
4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali, la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Art. 14 – Diritto alla portabilità

1. Il diritto alla portabilità dei dati di cui all'articolo 20 del "Regolamento" non si applica ai trattamenti svolti dalla Provincia necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso ente.

Art. 15 – Diritto di opposizione

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita la Provincia, compresa la profilazione sulla base di tali disposizioni.
2. La Provincia si astiene dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento, che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato, oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
3. L'opposizione è formulata per iscritto e inviata anche tramite posta elettronica.
4. L'interessato deve dimostrare la propria identità, inoltrando domanda corredata da documento di identità in corso di validità, anche via mail o mediante richiesta sottoscritta con firma digitale o equivalente trasmessa via PEC.
5. Da parte del Responsabile del trattamento dei dati oggetto dell'opposizione, il diritto di cui al comma 1 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

CAPO IV – I SOGGETTI DEL TRATTAMENTO E DELLA SICUREZZA DEI DATI

Art. 16 – Titolare del trattamento

1. Titolare del trattamento dei dati personali è la Provincia nel suo complesso.
2. L'articolazione organizzativa della Provincia e la formulazione degli incarichi assicurano le funzioni del titolare.
3. Il Titolare, tramite la propria complessiva articolazione:
   a) nomina il Responsabile della protezione dei dati;
   b) nomina quali Responsabili del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto della Provincia;
   c) assicura l'assolvimento delle proprie competenze creando adeguata articolazione interna, e garantendo risorse economiche, di personale, informatiche e formative.
4. Il Titolare può delegare ai Dirigenti pro-tempore dell'Ente, ai sensi dell'art. 2–*quaterdecies,* del D.lgs. 196/2003 e s.m.i., ogni più ampio potere in ordine al compimento di tutte le attività necessarie, utili o anche solo opportune al fine di individuare e nominare:
   a) i responsabili esterni al trattamento, di cui all'art. 28 Regolamento (UE) 2016/679, definiti come quei soggetti, persone fisiche o giuridiche, che trattano dati personali per conto del titolare del trattamento, in nome e per conto dell'Ente;
   b) i dipendenti interni nonché gli eventuali collaboratori (sia a tempo determinato sia con incarico autonomo) autorizzati al trattamento, in nome e per conto dell'Ente.

Art. 17 – Registri delle attività di trattamento

1. Il titolare del trattamento istituisce e aggiorna:
   - il *Registro delle attività del Titolare del trattamento;*
   - il *Registro delle attività del Responsabile del trattamento, in quanto nominato da soggetti esterni.*
2. I registri hanno i contenuti minimi previsti dalla Legge. Nei Registri possono essere inserite ulteriori informazioni rispetto a quelle minime previste dal Regolamento e dal Codice.
3. I Registri sono tenuti in forma telematica dal Titolare.
4. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere i Registri, di digitalizzarli e di integrali secondo le istruzioni impartite.

Art. 18 – Contitolari del trattamento

1. Si ha contitolarità del trattamento, ai sensi dell'art. 26 RPGD, quando due o più titolari determinano congiuntamente e in modo trasparente, mediante accordo interno, le finalità ed i mezzi del trattamento.
2. L'accordo definisce le responsabilità di ciascun titolare in merito all'osservanza degli obblighi derivanti dal 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 europea o statale specificatamente applicabile. Tale accordo può individuare un punto di contatto comune per gli interessati.
3. Con riferimento ai servizi connessi con il Sistema Informativo Bibliotecario della Provincia, offerti mediante convenzione o protocollo di intesa si ha contitolarità del trattamento tra la Provincia di Padova ed i Comuni aderenti.

Art. 19 – Responsabile esterno del trattamento

1. Qualora, a soggetti pubblici o privati esterni, siano affidati tramite delega o concessione o contratto lo svolgimento di compiti e/o servizi di competenza di questa Provincia da cui debba conseguire il trattamento di dati personali, il provvedimento o contratto di affidamento deve contenere una clausola di accettazione della nomina a Responsabile esterno del trattamento del legale rappresentante del soggetto pubblico o privato ovvero della persona fisica affidataria
2. Il Responsabile esterno del trattamento dei dati provvede a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare. La disciplina ed il livello di responsabilità sono contenuti in apposita separato atto di nomina, contenente l'obbligo di osservare le prescrizioni di cui al RGPD e alle altre fonti di diritto dell'Unione e dello Stato in materia di protezione dei dati personali nonché di consentire le verifiche sul rispetto delle predette disposizioni normative.
3. L'eventuale nomina da parte dei responsabili esterni di sub-responsabili del trattamento, è soggetta ad autorizzazione generica del titolare, nel rispetto degli stessi obblighi

contrattuali che legano il Titolare ed il Responsabile primario. L'autorizzazione può essere negata nel caso in cui il soggetto designato come sub-responsabile non dia sufficienti garanzie sul corretto trattamento.

4. Il trattamento dei dati da parte dei responsabili o sub-responsabili può essere assicurato solo da incaricati che operano sotto la diretta autorità del Responsabile o sub-responsabile stessi.
5. Nei casi di trattamento dei dati personali di cui ai commi precedenti il Dirigente, cui accede per competenza il servizio affidato, ha il potere di verificare che il soggetto esterno osservi le predette prescrizioni; mentre l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.
6. La periodicità delle predette verifiche, previste nell'atto di nomina, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento.
7. Delle operazioni di verifica e dei relativi esiti è dato riscontro mediante verbale, sottoscritto dal soggetto che effettua le verifiche e dal Responsabile esterno.

Art. 20 – Responsabile della protezione dati

1. La Provincia si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.
2. Il RPD può essere un dipendente a tempo indeterminato di questa Provincia, inquadrato in una categoria non inferiore alla D), se in possesso dei requisiti di cui al punto precedente. In tal caso viene designato con decreto del Presidente della Provincia.
3. Il RPD, di norma, è un soggetto esterno, persona fisica o persona giuridica, in possesso dei requisiti di cui al punto 1), scelto previa applicazione della vigente disciplina in materia di affidamento dei servizi. Esso assolve ai suoi compiti in base ad un contratto di servizio sottoscritto dal dirigente competente.
4. L'assenza di conflitti di interesse, anche potenziali, con l'esercizio dei propri compiti è strettamente connessa agli obblighi di indipendenza del RPD.
5. Nel contratto di servizio relativo all'affidamento dell'incarico di RPD devono essere riportati i compiti che lo stesso è tenuto a svolgere, tra cui almeno i seguenti:
   - Informare e fornire consulenza al Titolare o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonchè da altre disposizioni dell'Unione in materia di protezione dei dati;
   - Sorvegliare l'osservanza del Regolamento e di altre disposizioni dell'Unione, valutando i rischi di ogni trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
   - Collaborare con il Titolare/Responsabile del trattamento, ove necessario in merito alla valutazione di impatto sulla protezione dei dati (DPIA);

- Cooperare con il Garante privacy e fungere da punto di contatto per il garante su ogni questione connessa al trattamento;
- Supportare il Titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta del registro delle attività di trattamento;
- L'espletamento dei predetti compiti comporta le realizzazione delle seguenti attività consulenziali:
  - Analisi impatto dati trattati;
  - Analisi dei rischi effettivi e misure di ripristino;
  - Individuazione misure idonee;
  - Predisposizione documentazione privacy aggiornata al Regolamento 679/2016;
  - Supporto alla revisione e controllo della comunicazione verso l'esterno;
  - Predisposizione adeguamento documentazione interna al provvedimento del Garante in materia di utilizzo della rete da parte dei dipendenti;
  - Supporto alla creazione di informative interne ad uso degli incaricati del trattamento;
  - Formazione interna agli incaricati del trattamento ed ai responsabili del trattamento (per il numero di giornate indicate in sede di gara);
  - Revisione annuale informative interne ad uso degli incaricati del trattamento;
  - Revisione annuale documentazione da inviare dipendenti, fornitori e affidatari di servizi;
  - Invio circolari in caso di modifiche al Regolamento 679/2016;
  - Predisposizione di audit periodici per individuare i trattamenti svolti;
  - Assistenza per la realizzazione e la tenuta del Registro dei trattamenti del titolare e del responsabile del trattamento;
  - Definizione di un piano annuale delle attività che indichi, in relazione alle aree a maggior rischio in termini di protezione dati, un ordine di priorità degli interventi da comunicare al Titolare, sempre tenendo conto delle risorse disponibili.

6. Il Titolare/Responsabile del trattamento ed i dirigenti delegati si 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 delegati al trattamento che abbiano per oggetto questioni inerenti la protezione dei dati personali.
7. Il RPD rapporta lo svolgimento della propria funzione a linee guida, pareri, circolari, atti del Garante, e ad eventuali sopraggiunte fonti normative, e si adegua alle migliori prassi tecniche e amministrative.
8. Il RPD è tempestivamente e adeguatamente coinvolto nelle questioni riguardanti la protezione dei dati personali. A tal fine, il RPD partecipa alle riunioni periodiche di coordinamento che abbiano per oggetto questioni inerenti la protezione dei dati personali.
9. Al RPD viene dato adeguato supporto in termini di risorse strumentali (sede e attrezzature) e umane (dipendenti provinciali), costituite in gruppo di lavoro che lo coadiuvi

nell'espletamento dei suoi compiti; allo stesso viene garantito l'accesso ai servizi funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

10. E' obbligatorio richiedere il parere del RPD sulle decisioni che impattano sulla disciplina e sulla prassi da seguire nell'Ente in materia di protezione dei dati; qualora la decisione assunta determini condotte difformi dal parere del RPD, è necessario motivare specificamente tale decisione;
11. Il RPD, consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente, con proprio parere indica quali provvedimenti debbano essere adottati per porre rimedio ovvero per prevenire il ripetersi di tali violazioni.
12. Il titolare/responsabile del trattamento si assicura che il RPD non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti.
13. Il RPD non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti.
14. Il RPD riferisce direttamente al Presidente e al Segretario generale.
15. Gli interessati possono contattare direttamente il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
16. Il Responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o dello Stato.
17. 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

Art. 21 – Organizzazione del titolare

1. Il titolare assicura una organizzazione interna idonea a garantire la funzione prevista dalla Legge, anche tramite i propri strumenti di programmazione generale (DUP) e gestionale (PEG e piano degli obiettivi).
2. Il Presidente della Provincia pro tempore, in quanto rappresentante legale del titolare del trattamento, è competente ad adottare gli atti attuativi del presente regolamento.
3. Il direttore generale o, ove non nominato, il Segretario generale è competente a coordinare le attività trasversali volte ad assicurare una organizzazione del titolare tale da garantire l'assolvimento dei compiti attribuitegli dalla legge.

Art. 22 – Dirigenti

1. I dirigenti attuano i compiti delegati dal Titolare del trattamento, ai sensi del precedente art. 16, comma 4, e svolgono le seguenti funzioni:
   - adottano atti ed istruzioni operative per il rispetto delle misure indicate nei registri dei trattamenti per la protezione dei dati.
   - individuano eventuali attività di trattamento non previste all'interno dei registri delle attività di trattamento al fine di consentirne il costante aggiornamento;

- vigilano sulla azione dei soggetti autorizzati al trattamento, ponendo in essere adeguate azioni correttive in caso di riscontrate violazioni delle misure tecnico-organizzative indicate nei registri dei trattamenti;
- individuano i soggetti responsabili esterni del trattamento per conto del titolare, con conseguente definizione puntuale dei loro obblighi all'interno di apposito contratto/atto giuridico;
- coinvolgono i RPD in tutte le questioni riguardanti la protezione dei dati personali;
- garantiscono il rispetto dei diritti del soggetto interessato e forniscono le informative sul trattamento dei dati personali;
- consentono l'attività di formazione del personale autorizzato alle attività di trattamento dei dati personali;
- propongono nuove misure di sicurezza per il trattamento dei dati personali;
- nei documenti contrattuali che formalizzano obblighi giuridici con il fornitore/appaltatore inseriscono la clausola di accettazione della nomina a responsabile esterno del trattamento dei dati personali.

Art. 23 – Autorizzati al trattamento

1. I dirigenti autorizzano ai sensi del precedente art. 16, comma 4, i dipendenti interni nonché gli eventuali collaboratori (sia a tempo determinato sia con incarico autonomo) autorizzati al trattamento, in nome e per conto dell'Ente.
2. Sono parificati, ai fini del comma 1, anche i dipendenti in comando o distaccati presso l'Ente, eventuali tirocinanti o stagisti nonché personale di ditte esterne che, a qualsiasi titolo, presta la propria attività all'interno degli uffici della Provincia.
3. Gli autorizzati:
   - operano attenendosi alle istruzioni impartite, con particolare riferimento alla custodia degli atti e documenti analogici e digitali contenenti dati personali sensibili e giudiziari e alle relative misure di sicurezza;
   - trattano i dati personali per lo svolgimento delle funzioni istituzionali della Provincia, in conformità alle disposizioni per la protezione dei dati previste dal Regolamento Europeo 2016/679 e dalle disposizioni nazionali e del Regolamento provinciale di tempo in tempo vigenti;
   - provvedono:
     a) alla raccolta e registrazione per gli scopi inerenti l'attività istituzionale svolta;
     b) alla verifica in ordine alla pertinenza, completezza e non eccedenza delle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile del trattamento;
     c) alla conservazione, rispettando le misure di sicurezza predisposte al riguardo vigila che gli incaricati osservino la normativa in materia di trattamento dei dati.
4. Per ogni operazione di trattamento il subresponsabile garantisce la massima riservatezza.

Art. 24 – Amministratori del sistema informatico

1. La Provincia si avvale obbligatoriamente di amministratori del sistema informatico al fine di assicurare che il sistema informatico dell'Ente sia strutturato e gestito in modo da garantire le misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema.
2. Gli amministratore del sistema devono essere in possesso di titolo di studio specifico in informatica almeno di scuola media di secondo grado o laurea triennale e di comprovate conoscenze specialistiche tecniche e giuridiche in materia di sicurezza degli strumenti e dei programmi informatici per la protezione dei dati personali nonché della capacità di assolvere i compiti di competenza.
3. Con atto di nomina del Dirigente del Servizio Sistemi Informativi, può essere nominato Amministratore del sistema informatico un dipendente provinciale a tempo indeterminato inquadrato almeno nella categoria "C" ovvero, in caso di carenza di organico, un soggetto esterno, persona fisica. La designazione del soggetto esterno avviene tra quanti abbiano partecipato ad una apposita procedura ad evidenza pubblica e assolve i suoi compiti in base a un contratto di servizi sottoscritto dal competente Dirigente. L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti è strettamente connessa agli obblighi di autonomia e indipendenza dell'Amministratore di sistema.
4. Nell'atto ovvero nel contratto di servizio con cui è nominato Amministratore di sistema il dipendente provinciale o il soggetto esterno all'Ente devono essere riportati, altresì, tutti gli adempimenti e ciò che essi comportano sia sul piano delle procedure amministrative, che dell'organizzazione, che dell'adozione e verifica di ogni misura necessaria in materia di protezione dei dati personali dalle fonti di diritto europee e nazionali, dal "Gruppo di Lavoro europeo 29", dal Garante della Privacy, dalle disposizioni regolamentari e dalle direttive emanate dal Titolare del trattamento e dal RPD, nonché per conformarsi alla disciplina del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82/2004 e ss.mm.ii.
5. L'Amministratore di sistema cura i seguenti adempimenti:
    - gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate;
    - impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
    - registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema; impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per i Responsabili e gli Incaricati dei trattamenti di dati personali effettuati con strumenti elettronici nonché di quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzati;

- verificare costantemente che il Titolare del trattamento abbia adottato le misure tecniche e organizzative adeguate per la sicurezza informatica dei dati personali, provvedendo senza indugio agli adeguamenti eventualmente necessari, redigendo, se necessario, entro il 30 settembre di ogni anno una apposita relazione da inviare al Dirigente dell'Area Affari generali e Sistemi Informativi e al RPD dei dati in modo da attuare gli adempimenti amministrativi e contabili per la previsione nella successiva programmazione utile per la realizzazione delle ulteriori misure;
- suggerire al Titolare del trattamento e al RPD l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati atte a che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

6. In particolare l'Amministratore di sistema deve:
   - assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nel Disciplinare tecnico e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare ai soggetti incaricati del trattamento dei dati, svolgendo anche la funzione di custode delle copie delle credenziali;
   - custodire le parole chiave attribuite dagli incaricati del trattamento di dati personali con elaboratori elettronici e preservare con estrema attenzione il "cartellino delle credenziali di autenticazione" in modo da evitare accidentali aperture della busta ed evitare di aprire tali buste;
   - nel caso in cui il Titolare del trattamento o il Dirigente abbia la necessità indifferibile di accedere ad un elaboratore in caso di assenza o impedimento dell'incaricato che lo utilizza abitualmente, consentire al Titolare del trattamento o al Dirigente con una nuova parola chiave l'accesso all'elaboratore sul quale egli possa intervenire unicamente per necessità di operatività e sicurezza del sistema informativo; informare l'Incaricato del trattamento allorché rientri in servizio e consegnargli una nuova parola chiave diversa da quella consegnata al Responsabile del trattamento durante la sua assenza.
   - procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva ai soggetti interessati l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;
   - dotare e attivare nonché aggiornare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza e

protezione dei dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici, ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi;

- aggiornare periodicamente, con frequenza almeno annuale (oppure semestrale se si trattano dati sensibili o giudiziari), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- curare l'adozione e l'aggiornamento delle predette misure di sicurezza;
- impartire a tutti i soggetti che comunque svolgano trattamento dei dati istruzioni organizzative dirette al salvataggio quotidiano dei dati; prendere pertanto tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up; assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza;
- indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati allorché si provveda al loro reimpiego.

7. All'amministratore di sistema è fatto divieto di:
   - fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati; tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Responsabili del trattamento a conoscere i dati personali oggetto di trattamento;
   - fatto obbligo di dare tempestiva comunicazione al Titolare del trattamento, al RPD e ai Dirigenti dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati;
   - obbligato a osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici, degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta dei dati.
   - Il RPD procederà, entro il mese di settembre di ogni anno, alla verifica delle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Art. 25 – Misure di sicurezza del trattamento

1. Le misure di sicurezza sono determinate in relazione alle potenzialità organizzative della

Provincia, al livello di sviluppo tecnologico da essa acquisito, alle funzioni da assicurare e ai trattamenti da compiere.

2. Il titolare mette in atto misure tecniche ed organizzative 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 della probabilità del rischio e gravità per i diritti e le libertà delle persone fisiche.
3. Il responsabile del Servizio Sistemi Informativi, cui è conferito il compito di sovrintendere alle risorse del sistema operativo interno, ed i dirigenti, nell'ambito delle articolazioni organizzative cui sono preposti, in base alle risorse assegnate, in relazione allo sviluppo tecnologico e all'evoluzione del quadro normativo di riferimento, adeguano le disposizioni organizzative e le modalità di attuazione delle misure di sicurezza, alle disposizioni normative.
4. Le misure di sicurezza ricomprendono misure tecniche, di tipo informatico o tecnologico ai sensi della circolare AGID 2/2017, recante "Misure minime di sicurezza Ict per le pubbliche amministrazioni" e misure organizzative, di tipo procedurale o materiale.
5. Fra le misure tecniche rientrano:
   a) la pseudonimizzazione;
   b) la protezione informatica di dati e sistemi mediante:
      - cifratura: tecnica di protezione crittografica dei dati rilevante per minimizzare i rischi incombenti soprattutto in caso di accesso abusivo e perdita di dati;
      - misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali, comprese altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
      - sistemi di protezione (antivirus; firewall; antintrusione; altro) - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.
      - sistemi di autenticazione;
      - sistemi di allarme e rilevazione logistica: misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza.
6. Fra le misure organizzative di sicurezza rientrano:
      - la minimizzazione,
      - l'impiego di idonee armadiature e cassettiere;
      - disposizioni per la redazione dei provvedimenti amministrativi e tutela della privacy (prot.108730 del 31.07.2013);
      - formazione del personale;
      - inserimento nei contratti della clausola di accettazione a responsabile esterno;
      - il vigente disciplinare per l'utilizzo degli strumenti informatici;
      - il vigente manuale per la conservazione digitale;

- il vigente manuale per la gestione del protocollo informatico;
- delega del Titolare del trattamento ai Dirigenti per la nomina dei responsabili esterni e di autorizzazione al personale;
- lettere di autorizzazione al personale incaricato al trattamento;
- lettere di nomina ai responsabili esterni;
- nomina degli amministratori di sistema, interni ed esterni;
- le buone pratiche per non lasciare visibili dati personali sui luoghi di lavoro;
- sistemi di autorizzazione (all'ingresso in luoghi o all'impiego di documenti).

7. Vengono progressivamente introdotte procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
8. L'introduzione di misure di sicurezza avviene in una logica di progressivo sviluppo, partendo dallo stato esistente, e stabilendo misure di miglioramento, rapportate alla limitatezza delle risorse finanziarie, informative, tecnologiche e di personale.
9. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico correlati al codice.

Art. 26 – Comunicazione interna di dati personali

1. La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lettera 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.
2. I Dirigenti ed il personale autorizzato devono, comunque, rispettare le misure di sicurezza previste nel presente Regolamento, con particolare riguardo al trattamento delle specifiche categorie di dati personali e/o giudiziari.

Art. 27 – Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. Nel caso di trattamenti soggetti a valutazione di impatto, rimangono efficaci le modalità di trattamento e le valutazioni di impatto svolte dal titolare prima dell'adeguamento del presente regolamento alla normativa comunitaria, a prescindere dal documento nel quale sono contenuti, ferma la necessità di loro aggiornamento ove ne vengano mutate caratteristiche o contenuti.
2. Fermo restando quanto indicato dalla legge, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono specificati in documenti attuativi del presente regolamento.
3. 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 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;
- 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.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA a soggetto esterno.
5. 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.
6. Il Dirigente dell'Area Affari Generali e Sistemi Informativi fornisce supporto al Titolare per lo svolgimento della DPIA, ove sia interessato il sistema informativo.

Art. 28 – 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 dall'Ente.
2. Si individuano, tra rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, 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 e danno economico;
   - decifratura della pseudonimizzazione;
   - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
3. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, 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. 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;
- comportare rischi imminenti e con un'elevata probabilità di accadimento;
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni.

Art. 29 – Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative, oltre a quelle del Codice, in relazione alle norme vigenti. Il presente regolamento è strumento normativo cedevole rispetto alle disposizioni normative comunitarie e nazionali.