



**PROVINCIA
DI PARMA**

REGOLAMENTO PROVINCIALE
PER LA PROTEZIONE DEI DATI PERSONALI
in attuazione del Regolamento UE 2016/679
“Regolamento generale per la protezione dei dati”

Approvato con atto Consiglio Provinciale n. 22 del 04/06/2018

I N D I C E

articolo	rubrica
	Capo I Disposizioni generali e principi
1	Oggetto del regolamento
2	Definizioni
3	Finalità del trattamento
4	Principi applicabili al trattamento
5	Liceità del trattamento
6	Consenso dell'interessato
7	Trattamento dei dati sensibili
8	Trattamento dei dati giudiziari
	Capo II Diritti dell'interessato
9	Informativa, comunicazione e modalità trasparenti per l'esercizio dei diritti dell'interessato
10	Informativa per i dati da raccogliere presso l'interessato
11	Informativa per dati da ottenere da soggetti diversi dall'interessato
12	Diritto di accesso dell'interessato
13	Diritto di rettifica e integrazione
14	Diritto alla cancellazione (c.d. diritto all'oblio)
15	Diritto di limitazione del trattamento
16	Diritto alla portabilità dei dati
17	Diritto di opposizione
18	Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione
	Capo III Soggetti responsabili del trattamento e della sicurezza dei dati
19	Titolare del trattamento
20	Contitolari del trattamento
21	Responsabili del trattamento
22	Subresponsabili e Incaricati del trattamento
23	Amministratore del sistema informatico
24	Responsabile della protezione dei dati
25	Trattamento dei dati personali nei servizi esternalizzati
26	Comunicazione interna di documenti contenenti dati personale
27	Utilizzo di dati personali da parte dei componenti degli organi di governo e di controllo interno
	Capo IV Sicurezza dei dati personali
28	Misure per la sicurezza dei dati personali
29	Registro delle attività di trattamento del Titolare
30	Valutazione di impatto sulla protezione dei dati
31	Violazione dei dati personali
32	Entrata in vigore, pubblicazione e divulgazione del trattamento

CAPO I
DISPOSIZIONI GENERALI E PRINCIPI

Articolo 1
OGGETTO DEL REGOLAMENTO

1. Il presente Regolamento disciplina le misure procedurali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo n. 679 del 27 aprile 2016 "Regolamento generale sulla protezione dei dati" (RGPD), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali nonché alla libera circolazione di tali dati.
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 "Gruppo di Lavoro 29" nonché del Garante della Privacy, alle direttive impartite dal Titolare del trattamento, dai Responsabili del trattamento, dall'Amministratore del sistema informatico e dal Responsabile della protezione dei dati.

Articolo 2
DEFINIZIONI
(artt. 4, 9, 10 RGPD)

1. Ai fini del presente regolamento si intende per:
 1. «**Provincia**»: la Provincia di Parma, nella qualità il titolare del trattamento dei dati personali, le cui funzioni sono esercitate dai propri organi di governo nell'ambito delle rispettive competenze;
 2. «**Garante**»: l'Autorità di controllo ossia il Garante della Privacy;
 3. «**RGPD o REG. UE 2016/679**»: il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "Regolamento generale sulla protezione dei dati";
 4. «**Codice**»: il d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali";
 5. «**C**»: i "considerando" del Regolamento (UE) 2016/679;
 6. «**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; **(C26, C27, C30)**
 7. «**dati sensibili**»: 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; **(C51)**
 8. «**dati giudiziari**»: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
 9. «**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; **(C34)**
 10. «**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; **(C51)**
 11. «**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; **(C35)**
 12. «**interessato**»: la persona fisica titolare dei dati personali oggetto di trattamento;
 13. «**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;

14. «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)
 15. «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali 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; (C24, C30, C71-C72)
 16. «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a 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 che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)
 17. «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (C15)
 18. «**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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74)
 19. «**contitolari del trattamento**»: due o più titolari del trattamento che determinano congiuntamente, mediante un accordo interno, le finalità e i mezzi del trattamento;
 20. «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
 21. «**sub-responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali a cui fa ricorso il responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;
 22. «**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;
 23. «**responsabile della protezione dei dati**»: il dipendente del titolare o del responsabile del trattamento ovvero la persona fisica o giuridica estranea all'organizzazione del titolare o del responsabile del trattamento che svolge i compiti di cui all'art. 39 del REG. UE 2016/679 o ulteriori compiti affidati dal titolare del trattamento sulla base di un contratto di servizi;
 24. «**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.
 25. «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento;
 26. «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (C31)
 27. «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (C32, C33)
 28. «**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; (C85)
 29. «**Unione**»: l'Unione Europea;
 30. «**Stato**»: lo Stato italiano.
2. Per le definizioni non riportate nel precedente comma si rinvia all'elenco definizioni previste dall'art. 4 del RGPD.

Articolo 3
FINALITÀ DEL TRATTAMENTO
 (art. 3 RGPD)

1. I trattamenti dei dati personali sono eseguiti dalla Provincia per le seguenti finalità di pubblico interesse, stabilite dalle fonti normative che rispettivamente le disciplinano:
 - a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; rientrano in questo ambito i trattamenti dei dati personali compiuti per:
 - l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei seguenti settori organici:
 - a) pianificazione territoriale provinciale di coordinamento, nonché tutela e valorizzazione dell'ambiente, per gli aspetti di competenza;
 - b) 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;
 - c) programmazione provinciale della rete scolastica, nel rispetto della programmazione regionale;
 - d) raccolta ed elaborazione di dati, assistenza tecnico-amministrativa agli enti locali;
 - e) gestione dell'edilizia scolastica;
 - f) controllo dei fenomeni discriminatori in ambito occupazionale e promozione delle pari opportunità sul territorio provinciale.
 - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale o regionale, trasferite o delegate o comunque affidate alla Provincia in base alla vigente legislazione;
 - b) l'adempimento di un obbligo legale al quale è soggetta la Provincia;
 - c) l'esecuzione di un contratto con riguardo ai soggetti interessati;
 - d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Articolo 4
PRINCIPI APPLICABILI AL TRATTAMENTO
(art. 5 – C39, C74 - RGPD)

1. I dati personali sono trattati nel rispetto dei principi di : (C39)
 - a) «**liceità, correttezza e trasparenza**»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
 - b) «**limitazione delle finalità** »: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, prf. 1 del RGPD, considerato incompatibile con le finalità iniziali;
 - c) «**minimizzazione dei dati** »: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
 - d) «**esattezza**»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
 - e) «**limitazione della conservazione**»: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, prf. 1 del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;
 - f) «**integrità e riservatezza**»: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
 - g) «**responsabilizzazione**»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di provarlo. (C74)

2. Nelle ipotesi in cui disposizioni legislative, regolamentari o statutarie prevedano pubblicazioni obbligatorie, il responsabile del procedimento adotta le opportune misure atte a garantire la riservatezza dei dati personali a norma del RGPD, del “Codice della privacy” di cui al d.lgs. 30 giugno 2003.n. 196, del “Codice della trasparenza” di cui al d.lgs. 14 marzo 2013, n. 33 e ss.mm.ii., delle norme di tempo in tempo vigenti, e dei provvedimenti del Garante della Privacy.

Articolo 5

LICEITÀ DEL TRATTAMENTO

(art. 6 – C40→C46 - RGPD)

1. Il trattamento dei dati personali effettuato da questa Provincia é lecito soltanto per lo svolgimento delle proprie funzioni istituzionali e se:
 - a) l’interessato ha espresso il consenso al trattamento dei suoi dati personali per una o più specifiche finalità: tale condizione si applica alle pubbliche amministrazioni soltanto allorché le stesse dovessero svolgere trattamenti non attinenti ai propri compiti istituzionali di interesse pubblico o all’esercizio dei pubblici poteri attribuiti dal diritto dell’Unione o dello Stato;
 - b) il trattamento é necessario all’esecuzione di un contratto di cui l’interessato é parte o all’esecuzione di misure precontrattuali adottate su richiesta dello stesso interessato;
 - c) il trattamento é necessario per adempiere un obbligo legale al quale é soggetta questa Provincia; a tal fine lo Stato membro può mantenere o introdurre disposizioni più specifiche riguardo al trattamento, determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui agli articoli da 85 a 91 del RGPD. (art. 6, prf. 2, RGPD)
 - d) il trattamento é necessario per la salvaguardia degli interessi vitali dell’interessato o di un’altra persona fisica, se non trova applicazione alcuna delle altre predette condizioni;
 - e) il trattamento é necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui é investita questa Provincia; a tal fine lo Stato membro può mantenere o introdurre disposizioni più specifiche riguardo al trattamento, determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui agli articoli da 85 a 91 del RGPD. (art. 6, prf. 2, RGPD)
2. La base su cui si fonda il trattamento dei dati di cui alle lettere c) ed e) del comma 1 deve essere stabilita dal diritto dell’Unione o dello Stato.
3. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui alla lettera e) del comma 1, è necessaria per l’esecuzione di un compito svolto nel pubblico interesse o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l’applicazione delle norme del RGPD, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX dello stesso RGPD.
4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell’interessato o su un atto legislativo dell’Unione o dello Stato , al fine di verificare se il trattamento per un’altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l’altro: **(C50)**
 - a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell’ulteriore trattamento previsto;
 - b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l’interessato e il titolare del trattamento;

- c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del RGPD;
- d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 6
CONSENSO DELL'INTERESSATO
(art. 7 - da C40 a C46 – RGPD)

1. Questa Provincia non deve richiedere agli interessati il consenso per il trattamento dei loro dati personali allorché 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.
4. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
5. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 7
TRATTAMENTO DEI DATI SENSIBILI
(art. 9 RGPD)

1. È vietato trattare dati personali 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.
(C51)
2. Il divieto di cui al precedente comma non si applica se si verifica uno dei seguenti casi: **(C51, C52)**
 - a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al comma 1;
 - b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
 - c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
 - d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le

persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

- e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
 - f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
 - g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; **(C55, C56)**
 - h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al comma 3; **(C53)**
 - i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; **(C54)**
 - j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, del RGPD sulla base del diritto dell'Unione o nazionale, è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
3. I dati personali di cui al comma 1 possono essere trattati per le finalità di cui al comma 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o dello Stato o alle norme stabilite dagli organismi nazionali competenti. **(C53)**

Articolo 8

TRATTAMENTO DEI DATI GIUDIZIARI

(art. 10 RGPD)

1. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del RGPD 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.

CAPO II

DIRITTI DELL'INTERESSATO

Articolo 9

INFORMATIVA, COMUNICAZIONE E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

(art. 12 – C58, C60, C64 - RGPD)

1. La Provincia adotta misure appropriate per fornire all'interessato tutte le informazioni di cui ai successivi articoli 10 e 11 e le comunicazioni di cui agli articoli da 12 a 18 e all'articolo 29 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di

informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2. La Provincia agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18. Nei casi di cui all'articolo 11, paragrafo 2, del RGPD la Provincia non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che la Provincia dimostri che non è in grado di identificare l'interessato.
3. La Provincia fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 12 a 18 senza ingiustificato ritardo e, comunque, al più tardi **entro un mese** dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. La Provincia informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato. Se non ottempera alla richiesta dell'interessato, la Provincia informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
4. Le informazioni fornite ai sensi degli articoli 10 e 11 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 12 a 18 e dell'articolo 29 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:
 - a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
 - b) rifiutare di soddisfare la richiesta. Incombe alla Provincia l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
5. Fatto salvo l'articolo 11 del RGPD, qualora la Provincia nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 12 a 17, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.
6. Le informazioni da fornire agli interessati a norma degli articoli 10 e 11 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

Articolo 10

INFORMATIVA PER I DATI DA RACCOGLIERE PRESSO L'INTERESSATO

(art. 13 – C60, C62 - RGPD)

1. In caso di raccolta presso l'interessato di dati che lo riguardano, la Provincia fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
 - a) l'identità e i dati di contatto del titolare del trattamento ;
 - b) i dati di contatto del responsabile della protezione dei dati;
 - c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
 - d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, la Provincia fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
 - a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
 - b) 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 del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

- c) qualora il trattamento di dati non sensibili e non giudiziari sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento dei dati sensibili sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e il diritto dell'Unione o dello Stato abbia disposto l'irrevocabilità del divieto di trattare gli stessi dati sensibili previsto dal paragrafo 1 dell'articolo 9 del RGPD, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
 - d) il diritto di proporre reclamo a un'autorità di controllo;
 - e) se la comunicazione di 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 di tali dati;
 - f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del RGPD, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora la Provincia intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al comma 2.
4. I commi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 11

INFORMATIVA PER I DATI DA OTTENERE DA SOGGETTI DIVERSI DALL'INTERESSATO

(art. 14 – C60, C62 - RGPD)

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
- a) l'identità e i dati di contatto della Provincia;
 - b) i dati di contatto del responsabile della protezione dei dati;
 - c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
 - d) le categorie di dati personali in questione;
 - e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
2. Oltre alle informazioni di cui al comma 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
- a) il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
 - b) l'esistenza del diritto dell'interessato di chiedere alla Provincia l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
 - c) qualora il trattamento di dati non sensibili e non giudiziari sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento dei dati sensibili sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e il diritto dell'Unione o dello Stato abbia disposto l'irrevocabilità del divieto di trattare gli stessi dati sensibili previsto dal paragrafo 1 dell'articolo 9 del RGPD, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
 - d) il diritto di proporre reclamo a un'autorità di controllo;
 - e) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
 - f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del RGPD, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. La Provincia fornisce le informazioni di cui ai commi 1 e 2:
- a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

- b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
 - c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati.
4. Qualora la Provincia intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al comma 2.
5. I commi da 1 a 4 non si applicano se e nella misura in cui:
- a) l'interessato dispone già delle informazioni;
 - b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, del RGPD o nella misura in cui l'obbligo di cui al comma 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, la Provincia adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
 - c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato e prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
 - d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o dello Stato, compreso un obbligo di segretezza previsto per legge.

Articolo 12

DIRITTO DI ACCESSO DELL'INTERESSATO

(art. 15 – C63, C64 - RGPD)

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, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
- a) le finalità del trattamento;
 - b) le categorie di dati personali in questione;
 - c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
 - d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
 - e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
 - f) il diritto di proporre reclamo a un'autorità di controllo;
 - g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
 - h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del RGPD e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi, le cui tariffe sono determinate dal Presidente. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
3. Il diritto di ottenere una copia di cui al comma 2 non deve ledere i diritti e le libertà altrui.
4. L'istanza è formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
5. Il Responsabile del trattamento dei dati, competente per la materia relativa al trattamento medesimo, ovvero, su delega di quest'ultimo, l'incaricato del trattamento, provvede a soddisfare la richiesta dell'interessato nel più breve tempo possibile e comunque non oltre trenta giorni.

Articolo 13

DIRITTO DI RETTIFICA E INTEGRAZIONE

(art. 16 – C65 – art. 19 RGPD)

1. L'interessato ha il diritto di ottenere dalla Provincia la rettifica dei suoi dati personali inesatti nonché , tenuto conto delle finalità del trattamento, l'integrazione dei suoi dati personali incompleti, anche fornendo una dichiarazione integrativa. L'istanza di rettifica o integrazione é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
2. 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.
3. Dell'eseguita rettifica o integrazione ovvero della motivata inammissibilità é data tempestiva comunicazione all'interessato con raccomandata con avviso di ricevimento o con notifica a mani o tramite p.e.c..
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.

Articolo 14

DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

(art. 17 – C65, C66 – art. 19 - RGPD)

1. L'interessato ha il diritto di ottenere dalla Provincia la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e la Provincia ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
 - a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
 - b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), ovvero all'art. 9, prf. 2, lett. a), del RGPD e se non sussiste altro fondamento giuridico per il trattamento;
 - c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, del RGPD e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2, del RGPD;
 - d) i dati personali sono stati trattati illecitamente;
 - e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato cui è soggetto il titolare del trattamento;
 - f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1, del RGPD.
2. L'istanza é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
3. La Provincia, se ha reso pubblici dati personali ed è obbligata, ai sensi del comma 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento, che stanno trattando i dati personali, della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
4. I commi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
 - a) per l'esercizio del diritto alla libertà di espressione e di informazione;
 - b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
 - c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3, del RGPD;
 - d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del RGPD nella misura in cui il diritto di cui al comma 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
 - e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

5. 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.

Articolo 15

DIRITTO DI LIMITAZIONE DI TRATTAMENTO

(artt. 18 e 19 – C67 – RGPD)

1. L'interessato ha il diritto di ottenere dalla Provincia la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
 - a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario alla Provincia per verificare l'esattezza di tali dati personali;
 - b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
 - c) benché la Provincia non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
 - d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, del RGPD in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
2. Se il trattamento è limitato a norma del comma 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, oppure per tutelare i diritti di un'altra persona fisica o giuridica, o per motivi di interesse pubblico rilevante dell'Unione o dello Stato.
3. L'interessato che ha ottenuto la limitazione del trattamento a norma del comma 1 è informato dalla Provincia prima che detta limitazione sia revocata.
4. Il Responsabile del trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali, la limitazione 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.

Articolo 16

DIRITTO ALLA PORTABILITÀ DEI DATI

(art. 20 – C68 - RGPD)

1. Il diritto alla portabilità dei dati di cui all'articolo 20 del RGPD 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.

Articolo 17

DIRITTO DI OPPOSIZIONE

(art. 21 – C69, C70 - RGPD)

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. 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.

2. L'opposizione è formulata dall'interessato per iscritto ed è inviata alla Provincia anche per posta elettronica.
3. 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.

Articolo 18

PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE, COMPRESA LA PROFILAZIONE

(art. 22 – C71, C72 - RGPD)

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il comma 1 non si applica nel caso in cui la decisione:
 - a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
 - b) sia autorizzata dal diritto dell'Unione o dello Stato, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
 - c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al comma 2, lettere a) e c), la Provincia attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al comma 2 non si basano sulle categorie di dati sensibili di cui all'articolo 9, paragrafo 1, del RGPD, a meno che non siano applicabili l'articolo 9, paragrafo 2, lettere a) o g), del RGPD, e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

CAPO III

SOGGETTI RESPONSABILI DEL TRATTAMENTO E DELLA SICUREZZA DEI DATI

Articolo 19

TITOLARE DEL TRATTAMENTO

(art. 24 – C74, C78 - RGPD)

1. La Provincia di Parma è il titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee, gestite dagli uffici comunali. Per il trattamento di dati la Provincia può avvalersi anche di soggetti pubblici o privati esterni tramite un contratto di servizio o altro atto giuridicamente valido nel quale sono specificati le finalità e le modalità del trattamento, le categorie di dati da trattare, le responsabilità e i doveri facenti carico al soggetto che svolgerà il trattamento, determinandone la qualifica di contitolare o responsabile del trattamento.
2. Le funzioni attribuite alla Provincia dal diritto dell'Unione e dello Stato sono esercitate dai propri organi di governo (Consiglio provinciale, Presidente) nell'ambito delle rispettive competenze. Il Presidente rappresenta la Provincia nella qualità di titolare del trattamento.
3. La Provincia è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
4. La Provincia mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
5. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

6. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
7. 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 siano stati ottenuti presso lo stesso interessato.
8. 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, la Provincia deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "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 articolo 31.
9. Il Presidente provvede a:
 - a) designare i Responsabili del trattamento nelle persone dei Dirigenti e/o dei Responsabili di P.O. delle singole strutture in cui si articola l'organizzazione provinciale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;
 - b) nominare il Responsabile della protezione dei dati;
 - c) nominare l'Amministratore del sistema informatico;
 - d) a diramare le direttive necessarie per l'applicazione delle disposizioni del RGPD e del presente regolamento, sentiti il Responsabile della protezione dei dati, il Segretario Generale, l'Amministratore del sistema informatico e i Responsabili del trattamento.
10. Nelle convenzioni, nelle concessioni, nei contratti, negli incarichi professionali o in altri strumenti giuridici consentiti dalla legge con cui è affidata a soggetti esterni alla Provincia la gestione di attività e/o servizi per conto di questa Amministrazione provinciale, è prevista espressamente la nomina degli stessi soggetti affidatari quali responsabili del trattamento dei dati personali connessi alle attività istituzionali affidate. Qualora negli atti vigenti manchi tale previsione, dovrà essere effettuata un'opportuna operazione di adeguamento.
11. L'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente è pubblicato, a cura del Responsabile della Trasparenza, in apposita sezione del sito istituzionale, aggiornandolo periodicamente.
12. La Provincia favorirà l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Articolo 20

CONTITOLARI DEL TRATTAMENTO

(art. 26 – C79 - RGPD)

1. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata alla Provincia da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente e in modo trasparente, mediante accordo interno, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD.
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.

Articolo 21
RESPONSABILI DEL TRATTAMENTO
(art. 28 – C81 - RGPD)

1. La Provincia si avvale obbligatoriamente di più Responsabili del trattamento, designati dal Presidente, di norma, entro tre mesi dalla data della sua proclamazione. La designazione avviene con il decreto di attribuzione delle funzioni dirigenziali o con separato decreto, nel quale sono tassativamente previsti:
 - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
 - il tipo di dati personali oggetto di trattamento e le categorie di interessati;
 - gli obblighi ed i diritti del Titolare del trattamento.
2. Sino alla designazione di cui al comma 1 , si intende prorogata di diritto la designazione dei Responsabili del trattamento in carica al momento della predetta proclamazione. Tale proroga é valida anche a seguito della nomina di un Commissario che sostituisca tutti gli organi di governo dell’Ente, salvo che lo stesso Commissario non ritenga necessario designare nuovi Responsabili del trattamento ovvero sostituire tutti o alcuni dei Responsabili del trattamento in carica all’atto della sua nomina.
3. Devono essere designati Responsabili del trattamento dei dati personali, contenuti in tutte le banche dati esistenti nell’articolazione organizzativa di rispettiva competenza, i Dirigenti delle strutture di massima dimensione in cui si articola l’organizzazione della Provincia. Possono essere designati, altresì, Responsabili del trattamento i Funzionari cui é attribuita la Posizione Organizzativa, limitatamente alle banche dati di propria competenza .
4. Il Responsabile del trattamento deve essere in grado, anche attraverso una adeguata preventiva formazione, di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui al successivo articolo 28, rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
5. La Provincia può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 4, stipulando **atti giuridici in forma scritta**, che specifichino 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.
6. Gli atti che disciplinano il rapporto tra il Titolare del trattamento e il Responsabile del trattamento devono in particolare contenere quanto previsto dall’art. 28, p. 3, del RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
7. Qualora un Responsabile del trattamento si assenti o sia impedito per un prolungato periodo di tempo superiore a trenta giorni, il Presidente provvede alla sua sostituzione temporanea.
8. E’ consentita la nomina 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 del trattamento e il Responsabile del trattamento primario, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD. Se il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile primario conserva nei confronti del Titolare del trattamento l’intera responsabilità dell’adempimento degli obblighi del sub-responsabile.
9. Le operazioni di trattamento possono essere effettuate solo da sub-responsabili o da incaricati che operano sotto la diretta autorità del Responsabile del trattamento, attenendosi alle istruzioni loro impartite per iscritto dallo stesso Responsabile, le quali istruzioni individuano specificatamente l’ambito del trattamento consentito.
10. Il Responsabile del trattamento risponde, anche dinanzi al Titolare del trattamento, dell’operato del sub-responsabile del trattamento e degli incaricati del 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 ha vigilato in modo adeguato sull’operato del sub-responsabile e dell’incaricato del trattamento.
11. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

12. Il Responsabile del trattamento provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare del trattamento, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare deve provvedere:
- a) a tenere aggiornato il registro delle categorie di attività di trattamento svolte per conto del Titolare;
 - b) ad adottare le misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
 - c) ad autorizzare i dipendenti appartenenti alla sua struttura ad accedere ai dati personali al fine di svolgere il trattamento afferente i rispettivi compiti istituzionali;
 - d) a sensibilizzare e formare il personale che partecipa ai trattamenti in materia di protezione dei dati personali, fornendo le istruzioni per il corretto trattamento dei dati personali, e a controllare che le attività di trattamento, con particolare riferimento alle operazioni di comunicazione e diffusione, svolte dagli incaricati, siano conformi alle norme del RGPD;
 - e) a collaborare con il Titolare al fine di definire la valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
 - f) a informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;
 - g) a curare le informative di cui agli articoli 13 e 14 del RGPD da fornire agli interessati, predisponendo la necessaria modulistica o determinando altre forme idonee di informazione inerenti i trattamenti di competenza della propria struttura organizzativa, facendo, in presenza di dati sensibili, espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento;
 - h) a curare l'eventuale raccolta del consenso degli interessati per il trattamento dei dati sensibili qualora il loro trattamento non sia previsto da una specifica norma di legge;
 - i) ad adottare le misure necessarie per facilitare l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD;
 - j) a stabilire le modalità di gestione e le forme di responsabilità relative a banche dati condivise da più articolazioni organizzative, d'intesa con gli altri responsabili; in caso di mancato accordo tra i Responsabili, decide il Segretario Generale, sentiti gli stessi Responsabili competenti;
 - k) a stipulare gli accordi con altri soggetti pubblici o privati per l'esercizio del diritto di accesso alle banche-dati nei limiti previsti dalle disposizioni legislative e regolamentari.

Articolo 22

SUBRESPONSABILI E INCARICATI DEL TRATTAMENTO INTERNI ALL'ENTE

(art. 29 – C81 - RGPD)

1. Il Responsabile può nominare subresponsabili, da individuarsi, di norma, nel personale incaricato di posizione organizzativa, affinché lo supportino nell'attuazione della normativa in materia di trattamento dei dati, e nello svolgimento dei compiti previsti dal precedente art.21.
2. Il subresponsabile:
 - opera sotto l'autorità del Responsabile del trattamento , 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;
 - tratta 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,
 - provvede:
 - alla raccolta e registrazione per gli scopi inerenti l'attività istituzionale svolta;
 - 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;
 - alla conservazione, rispettando le misure di sicurezza predisposte al riguardo
 - vigila che gli incaricati osservino la normativa in materia di trattamento dei dati.
3. Per ogni operazione di trattamento il subresponsabile garantisce la massima riservatezza.

4. Nel caso di allontanamento anche temporaneo dalla propria postazione di lavoro, il sub responsabile verifica che non vi sia la possibilità per chiunque non sia autorizzato all'accesso ai dati di accedere alle banche dati e/o dati personali per i quali è in corso un qualsiasi tipo di trattamento.
5. Le comunicazioni e diffusioni a soggetti diversi dagli interessati devono essere svolte nel pieno rispetto delle norme che lo disciplinano.
6. Incaricati del trattamento sono i soggetti interni a questa Provincia – componenti degli organi di governo e di controllo, dirigenti (ove non designati come Responsabili) e dipendenti provinciali – che hanno accesso a dati personali ovvero agiscono sotto l'autorità del titolare del trattamento o dei responsabili del trattamento.
7. Gli Incaricati del trattamento non possono svolgere operazioni di trattamento dei dati personali se non istruiti in tal senso dal Responsabile del trattamento.
8. I dipendenti provinciali sono designati Incaricati del trattamento e autorizzati al trattamento dei dati personali con formale provvedimento del Responsabile del trattamento competente per la struttura organizzativa in cui sono inseriti gli stessi dipendenti; in tale provvedimento sono indicati: i procedimenti amministrativi per lo svolgimento dei quali è indispensabile il trattamento dei dati personali; le finalità del trattamento; le categorie di dati personali da trattare; le operazioni di trattamento eseguibili, con particolare riferimento alla comunicazione e alla diffusione dei dati sensibili e giudiziari; gli eventuali limiti al trattamento; le misure di sicurezza da adottare da parte degli stessi Incaricati. Tali indicazioni possono essere formulate anche con rinvio al registro del trattamento, nella parte relativa ai trattamenti da attribuire. Le predette designazione e autorizzazione nonché le citate indicazioni del trattamento possono essere stabilite anche con un atto distinto dal contratto individuale di lavoro. Tale atto deve essere notificato al dipendente interessato, il quale non può esimersi dalla sua accettazione e attuazione.
9. I dipendenti possono essere individuati quali Incaricati del trattamento nominativamente ovvero con riferimento alla categoria di inquadramento o al profilo professionale o alla collocazione nell'organizzazione del servizio o dell'ufficio.
10. I dipendenti incaricati del trattamento operano sotto l'autorità dei Responsabili del trattamento, attenendosi alle istruzioni impartite per iscritto, con particolare riferimento alla custodia degli atti e documenti analogici e digitali contenenti dati personali sensibili e giudiziari e alle relative misure di sicurezza.
11. Agli incaricati compete, in relazione al trattamento dei dati personali provvedere:
 - al trattamento dei dati personali per lo svolgimento delle funzioni istituzionali della Provincia, in conformità alle disposizioni del RGPD;
 - alla raccolta e registrazione per gli scopi inerenti l'attività istituzionale svolta da ciascuno;
 - alla verifica in ordine alla loro pertinenza, completezza e non eccedenza delle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal responsabile del trattamento;
 - alla conservazione, rispettando le misure di sicurezza predisposte al riguardo.
12. Per ogni operazione di trattamento è da garantire la massima riservatezza.
13. Nel caso di allontanamento anche temporaneo dalla propria postazione di lavoro, l'incaricato verifica che non vi sia possibilità per chiunque non sia autorizzato all'accesso ai dati di accedere alle banche-dati e/o ai dati personali per i quali è in corso un qualsiasi tipo di trattamento.
14. Le comunicazioni e le diffusioni a soggetti diversi dagli interessati devono essere svolte nel pieno rispetto delle norme che le disciplinano.
15. Il flusso di dati, per ragioni di servizio, tra Titolare del trattamento, Responsabili del trattamento, Subresponsabili, Incaricati del trattamento, Amministratore del sistema informatico, il Responsabile della protezione dei dati, Segretario Generale, componenti degli organi di governo e di controllo interno non costituisce "comunicazione" in senso tecnico quale operazione di trattamento; ne consegue che tale flusso non è soggetto ai limiti previsti per tale operazione di trattamento.

Articolo 23

AMMINISTRATORE DEL SISTEMA INFORMATICO

(Garante Privacy provvedimento del 25.6.2009)

1. Al fine di ottemperare a quanto disposto dal Garante della Privacy con il provvedimento datato 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" come modificato con successivo provvedimento datato 25/06/2009, la Provincia si avvale obbligatoriamente di un amministratore del sistema informatico al fine di assicurare che il sistema informatico di questo 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. L'amministratore del sistema deve 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. Amministratore del sistema informatico può essere designato, con decreto del Presidente, un dipendente provinciale a tempo indeterminato inquadrato almeno nella categoria "C" ovvero, nel caso di mancanza di un dipendente, un soggetto esterno, persona fisica o soggetto giuridico. La designazione da parte del Presidente 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 designato 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 Responsabile della protezione dei dati, nonché per conformarsi alla disciplina del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82/2004 e ss.mm.ii., in particolare la cura dei seguenti adempimenti:
 - a) gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate;
 - b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
 - c) 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;
 - d) 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 entro il 30 settembre di ogni anno una apposita relazione da inviare al Presidente, al Segretario Generale e al Responsabile per la protezione dei dati in modo da attuare gli adempimenti amministrativi e contabili per la previsione nella successiva programmazione utile per la realizzazione delle ulteriori misure;
 - e) suggerire al Titolare del trattamento e ai Responsabili del trattamento 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;

Più specificamente, l'Amministratore di sistema dovrà:

- 1) 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 Responsabili e agli Incaricati del trattamento dei dati, svolgendo anche la funzione di custode delle copie delle credenziali; Più specificamente dovrà:
 - 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 Responsabile del trattamento abbia la necessità indifferibile di accedere ad un elaboratore in caso di assenza o impedimento dell'incaricato che lo utilizza abitualmente, consentire al Responsabile del trattamento 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.
- 2) 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;
 - 3) 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;
 - 4) 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;
 - 5) curare l'adozione e l'aggiornamento delle predette misure di sicurezza;
 - 6) 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;
 - 7) adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
 - 8) predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza ;
 - 9) 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;
5. All'Amministratore del sistema informatico è :
 - a) 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;
 - b) fatto obbligo di dare tempestiva comunicazione al Titolare e ai Responsabili del trattamento interessati nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati;
 - c) 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.
 6. Il Responsabile della protezione dei dati 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.

Articolo 24
RESPONSABILE DELLA PROTEZIONE DEI DATI
 (artt. 37, 38, 39 – C97 - RGPD)

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 Responsabile della protezione è designato con decreto del Presidente non oltre sei mesi dalla data della sua proclamazione.
3. Responsabile della protezione dei dati può essere designato un dipendente a tempo indeterminato di questa Provincia inquadrato in una categoria non inferiore alla D) ovvero un soggetto esterno, persona fisica o soggetto giuridico. La designazione da parte del Presidente 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 servizio sottoscritto dal Dirigente competente. L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti è strettamente connessa agli obblighi di indipendenza del RPD.
4. Il Dirigente competente in materia di Trasparenza provvede, tempestivamente, a che i dati identificativi e di contatto del Responsabile della protezione dei dati siano:
 - pubblicati nel sito web istituzionale dell'Ente, rendendoli accessibili da un apposito link;
 - comunicati al Garante della Privacy;
 - comunicati ai componenti degli organi di governo, a tutti i dirigenti e dipendenti provinciali, ai componenti degli organi di controllo interni.
5. Sino alla designazione del nuovo RPD si intende prorogata di diritto la designazione del Responsabile della protezione dei dati in carica al momento della predetta proclamazione. Tale proroga è valida anche a seguito della nomina di un Commissario che sostituisca tutti gli organi di governo dell'Ente, salvo che lo stesso Commissario non ritenga necessario designare un nuovo Responsabile della protezione dei dati ovvero sostituire il Responsabile in carica all'atto della sua nomina.
6. Nell'atto di designazione del soggetto interno all'Ente ovvero nel contratto di servizio relativi all'affidamento dell'incarico di RPD devono essere riportati i compiti che lo stesso è tenuto a svolgere, tra cui almeno i seguenti:
 - a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o dello Stato relative alla protezione dei dati; in tal senso il RPD indica al Titolare e/o ai Responsabili del trattamento 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, di altre disposizioni dell'Unione o dello Stato relative alla protezione dei dati nonché delle politiche del titolare del trattamento o dei responsabili del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; 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 dai Responsabili del trattamento;
 - d) fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD; il Titolare del trattamento, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;
 - e) verificare e relazionare, entro il mese di settembre di ogni anno, riguardo alle 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.
 - f) 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 del RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione.
7. Nell'eseguire i propri compiti il Responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. A tali fini il RPD procede a valutare la mappatura delle aree di attività fatta dai competenti uffici, e ne valuta il grado

di rischio in termini di protezione dei dati, determinandone un elenco in ordine decrescente di gravità, in modo da definire 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 e ai Responsabili del trattamento.

8. Il Titolare del trattamento e i Responsabili del trattamento 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 Responsabili del trattamento che abbiano per oggetto questioni inerenti la protezione dei dati personali;
 - il RPD deve ricevere tempestivamente, tramite posta elettronica, dal Titolare e dai Responsabili del trattamento tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da essere edotto sulla evoluzione della gestione in materia e da poter rendere una consulenza idonea;
 - é 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;
 - 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.
9. Il RPD è tenuto a manifestare il proprio dissenso alle decisioni o ai provvedimenti o ai comportamenti incompatibili con il RGPD adottati o tenuti dai componenti degli organi di governo e di controllo nonché degli organi di gestione e dei dipendenti ogni qual volta ne venga a conoscenza, dandone comunicazione al Presidente, al Segretario generale, ai Responsabili del trattamento interessati dai rilievi e, ove necessario, all'Amministratore del sistema informatico. I Responsabili del trattamento qualora non condividano i rilievi formulati dal RPD, comunicano a quest'ultimo, al Presidente e al Segretario Generale le proprie osservazioni. Il RPD dirama le direttive utili a prevenire il ripetersi delle violazioni rilevate.
10. Il Titolare del trattamento e i Responsabili del trattamento sostengono il Responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 del RGPD, fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. In particolare é assicurato al RPD:
 - supporto attivo per lo svolgimento dei compiti da parte dei Responsabili del trattamento, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg, di Piano della performance e di Piano della formazione;
 - tempo sufficiente per l'espletamento dei compiti affidati al RPD se designato all'interno all'Ente;
 - supporto adeguato 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;
 - accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.
11. Il titolare del trattamento e i responsabili del trattamento si assicurano che il Responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti.
12. Il Responsabile della protezione dei dati non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti.
13. Il Responsabile della protezione dei dati riferisce direttamente al Presidente e al Segretario generale.
14. 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
15. 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.
16. Il Responsabile della protezione dei dati può svolgere altri compiti e funzioni.

Articolo 25

TRATTAMENTO DI DATI PERSONALI NEI SERVIZI ESTERNALIZZATI

1. Nell' ipotesi che 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 prevedere norme specifiche attraverso le quali si

provvede: a nominare il legale rappresentante del soggetto pubblico o privato ovvero la persona fisica affidatario quale sub-responsabile del trattamento dei dati personali per la durata dell'affidamento; ad obbligare il soggetto affidatario ad 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; a consentire le verifiche sul rispetto delle predette disposizioni normative.

2. Nelle ipotesi di trattamento dei dati personali di cui al precedente comma, il Responsabile del trattamento della massima struttura organizzativa della Provincia competente per materia, in relazione al compito e/o al servizio affidato, ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; e l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.
3. La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, 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.
4. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Responsabile del trattamento e dai soggetti presenti a ciascuna verifica.

Articolo 26

COMUNICAZIONE INTERNA DI DOCUMENTI CONTENENTI 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. Il Responsabile del trattamento può tuttavia disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione concerna dati sensibili e/o giudiziari.

Articolo 27

UTILIZZO DI DATI DA PARTE DEI COMPONENTI GLI ORGANI DI GOVERNO E DI CONTROLLO INTERNO

1. Il Presidente, i Consiglieri provinciali nonché i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti da questa Provincia, contenenti dati personali detenuti dall'Amministrazione provinciale, nei limiti e con le modalità previsti dalle disposizioni di legge e di regolamenti.
2. Le notizie e le informazioni così acquisite devono essere utilizzate esclusivamente per le finalità pertinenti alle rispettive competenze, rispettando il divieto di divulgazione dei predetti documenti nonché l'obbligo della segretezza del loro contenuto.

CAPO IV

SICUREZZA DEI DATI PERSONALI

Articolo 28

MISURE PER LA SICUREZZA DEI DATI PERSONALI

(art. 32 – C83 - RGPD)

1. Il Titolare e i Responsabili del trattamento nonché l'Amministratore del sistema informatico e il Responsabile della protezione dei dati provvedono, per quanto di rispettiva competenza, all'adozione e alla dimostrazione di attuazione concreta di misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare

la continua riservatezza, integrità, disponibilità e resistenza dei sistemi e dei servizi con cui sono trattati i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal servizio cui è preposto ciascun Responsabile del trattamento:
 - sistemi di autenticazione, autorizzazione e protezione (antivirus; firewall; antintrusione; altro);
 - misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4. La conformità del trattamento dei dati al RGPD 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 e i Responsabili del trattamento nonché l'Amministratore del sistema informatico e il Responsabile della protezione dei dati 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.
6. I nominativi e i dati di contatto del Titolare e dei Responsabili del trattamento nonché dell'Amministratore del sistema informatico e del Responsabile della protezione dei dati sono pubblicati sul sito web istituzionale della Provincia, sezione "Amministrazione trasparente".
7. I responsabili del trattamento provvedono, nell'ambito dei propri poteri di controllo, a effettuare periodiche verifiche sulla corretta applicazione della normativa in materia di trattamento dei dati personali nell'ambito delle articolazioni organizzative cui sono preposti, in accordo con i controlli specifici effettuati dal responsabile della protezione dei dati.
8. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili e giudiziari per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).
9. Tutte le verifiche sulla corretta applicazione della normativa in materia di trattamento dei dati personali vengono documentate.

Articolo 29

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL TITOLARE- REGISTRI DEI SINGOLI RESPONSABILI

(art. 30 – C82 - RGPD)

1. E' istituito il Registro delle attività di trattamento svolte dal Titolare del trattamento, sul quale sono annotate almeno le seguenti informazioni:
 - a) il nome ed i dati di contatto della Provincia, del Presidente e del RPD;
 - b) le finalità del trattamento;
 - c) 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;
 - d) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
 - e) la descrizione delle categorie di interessati;
 - f) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
 - g) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
 - h) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
 - i) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il Registro è tenuto dal Titolare in forma telematica, unitamente al Registro delle categorie delle attività trattate dai Responsabili del trattamento di cui al successivo art. 30; nello stesso possono essere inserite ulteriori

informazioni tenuto conto delle dimensioni organizzative dell'Ente. In calce al registro andranno indicati i dati attinenti ai rischi rilevati, alla loro ponderazione e alle rispettive misure individuate.

3. Il Titolare del trattamento può delegare la tenuta del predetto Registro unitario a un solo Responsabile del trattamento ovvero al RPD, sotto la responsabilità del medesimo Titolare.
4. Il Registro del Titolare è la risultanza dei singoli registri dei responsabili dei trattamenti, previsti dall'art.30, paragrafo 2, del RGPD, redatti conformemente agli schemi di cui agli allegati A) e B) (o schemi equivalenti) al presente regolamento. 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.
5. Il Registro deve essere aggiornato annualmente entro il termine e in conformità alle direttive diramate dal Responsabile della protezione dei dati, il quale è tenuto a comunicare, entro trenta giorni successivi al predetto termine, le eventuali inadempienze al presidente e al Segretario Generale per le eventuali responsabilità dirigenziali e disciplinari che ne conseguono

Articolo 30

VALUTAZIONI DI IMPATTO SULLA PROTEZIONE DEI DATI

(artt. 35 e 36 – C84, C89, C93, C94, C95, C96 - RGPD)

1. Nel caso in cui una tipologia 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 valutazione dell'impatto del medesimo trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA, si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, paragrafi 4-6, del RGDP.
3. Fermo restando quanto indicato dall'art. 35, paragrafo 3, del RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
 - a) trattamenti valutativi o di attribuzione di punteggi, 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 analogo 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 del 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, sentito il Responsabile della protezione dei dati e l'Amministratore del sistema informatico, ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

- 4. Il Titolare del trattamento garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA al Responsabile della protezione dei dati ovvero ad altro soggetto, interno o esterno alla Provincia.

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, se gli viene affidato tale incombenza da parte del Titolare del trattamento, provvede allo svolgimento della DPIA ovvero, se non gli compete la predetta incombenza, monitora lo svolgimento della DPIA.

I Responsabili del trattamento collaborano e assistono il Titolare del trattamento e il Responsabile della protezione dei dati nella conduzione della DPIA, redigendo per quanto di competenza il Registro unitario di cui al precedente articolo 29 e fornendo ogni informazione necessaria.

L'Amministratore del sistema informatico fornisce il necessario supporto al Titolare per lo svolgimento della DPIA.

- 5. Il Responsabile della protezione dei dati 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.

L'Amministratore del sistema informatico può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

- 6. La DPIA non è necessaria nei casi seguenti:

- a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del RGDP;
- b) 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;
- c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- d) 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.

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

- 8. 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 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.
9. Il Titolare del trattamento 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.
10. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento, se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.
11. 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.
12. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Articolo 31

VIOLAZIONE DEI DATI PERSONALI

(artt. 33 e 34 – C85, C86, C87, C88 - RGPD)

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 Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
 - a) danni fisici, materiali o immateriali alle persone fisiche;
 - b) perdita del controllo dei dati personali;
 - c) limitazione dei diritti, discriminazione;
 - d) furto o usurpazione d'identità;
 - e) perdite finanziarie, danno economico o sociale;
 - f) decifratura non autorizzata della pseudonimizzazione;
 - g) pregiudizio alla reputazione;
 - h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
 - riguardare categorie particolari di dati personali;
 - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
 - comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
 - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 del RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33.
6. Il Titolare del trattamento 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 33

ENTRATA IN VIGORE, PUBBLICAZIONE E DIVULGAZIONE DEL REGOLAMENTO

1. L'efficacia del presente regolamento decorre dal giorno in cui diviene esecutiva la deliberazione con cui è stato approvato.
2. Il presente regolamento, divenuto esecutivo, è pubblicato nel sito web istituzionale della Provincia.
3. Il presente regolamento è trasmesso, per opportuna conoscenza, ai componenti degli organi di governo e degli organi di controllo interni, al segretario provinciale, ai dirigenti, i quali ultimi ne forniscono copia a tutti i sub-responsabili del trattamento e a tutti gli incaricati del trattamento.

TABELLA A INFORMAZIONI SUI TRATTAMENTI SVOLTI DA CIASCUN SERVIZIO

Legenda:

- Regolamento UE 2016/679 del Parlamento Europeo, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito RGSP);
- Regolamento Provinciale per la protezione dei dati personali, approvato con deliberazione del Consiglio Provinciale n° del (di seguito Reg. provinciale);

Finalità Art 3 Reg. Provinciale	<p>I trattamenti dei dati personali sono eseguiti dalla Provincia per le seguenti finalità di pubblico interesse, stabilite dalla fonti normative che rispettivamente le disciplinano:</p> <p>a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; rientrano in questo ambito i trattamenti dei dati personali compiuti per:</p> <p>a) pianificazione territoriale provinciale di coordinamento, nonché tutela e valorizzazione dell'ambiente, per gli aspetti di competenza;</p> <p>b) 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;</p> <p>c) programmazione provinciale della rete scolastica, nel rispetto della programmazione regionale;</p> <p>d) raccolta ed elaborazione di dati, assistenza tecnico-amministrativa agli enti locali;</p> <p>e) gestione dell'edilizia scolastica;</p> <p>f) controllo dei fenomeni discriminatori in ambito occupazionale e promozione delle pari opportunità sul territorio provinciale.</p> <p>b) l'esecuzione di un contratto con riguardo ai soggetti interessati;</p> <p>c) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.</p>										
Categorie di trattamento Art 4 par 1 nr.2) RGDP Art 2 reg. Provinciale	<p>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.</p>										
Natura dato	<p>Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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;</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center; width: 5%;">P</td> <td style="width: 35%;">Dato personale (non sensibile e non giudiziario)</td> <td></td> </tr> <tr> <td style="text-align: center;">S</td> <td>Dato Sensibile Art. 9 RGDP</td> <td>È vietato trattare dati personali 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.</td> </tr> <tr> <td style="text-align: center;">G</td> <td>Dato personale relativo a condanne penali e reati Art. 10 RGDP</td> <td>Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica</td> </tr> </table>		P	Dato personale (non sensibile e non giudiziario)		S	Dato Sensibile Art. 9 RGDP	È vietato trattare dati personali 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.	G	Dato personale relativo a condanne penali e reati Art. 10 RGDP	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica
P	Dato personale (non sensibile e non giudiziario)										
S	Dato Sensibile Art. 9 RGDP	È vietato trattare dati personali 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.									
G	Dato personale relativo a condanne penali e reati Art. 10 RGDP	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica									
Interessato Art. 2 comma 1 punto 12) Reg Provinciale	<p>La persona fisica titolare dei dati personali oggetto di trattamento</p>										
Destinatario Art. 4 paragrafo 1 nr. 9) RGDP Art. 2 comma 1 punto 26) Reg Provinciale	<p>La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.</p>										
Termine per la cancellazione Considerando 39 RGDP	<p>I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica.</p>										
Eventuale trasferimento di dati personali verso un Paese terzo od una Organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e per i trasferimenti di cui all'art.49, comma secondo Reg UE 2016/679, la documentazione delle garanzie adeguate											

Servizio

Ufficio

Dirigente _____

Responsabile del Trattamento _____ (Art. 21 Reg Provinciale)

Subresponsabile-----

Ufficio _____
 Indirizzo _____
 Recapiti mail _____ tel 0521 _____

TRATTAMENTI

Codifica	Breve Descrizione	Natura del Dato			Fonte Normativa	Codifica	Breve Descrizione	Natura del Dato			Fonte Normativa
		P	S	G				P	S	G	
n.b.d.						n.b.d.+4					
n.b.d.+1						n.b.d.+5					
n.b.d.+2						n.b.d.+6					
n.b.d.+3						n.b.d.+7					

La scheda NON sarà unica per tutti i trattamenti dell'ufficio, ma solo per trattamenti analoghi, quelli che hanno finalità, categoria, modalità, destinatari, incaricati uguali.

Attività/Trattamento	Finalità (Art. 3 Reg. Provinciale)	Categorie di trattamento e natura dato 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.	Modalità di trattamento	Categorie interessati	Categorie destinatari	Termine ultimo previsto per la cancellazione	Eventuale trasferimento di dati personali verso un Paese terzo od una Organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e per i trasferimenti di cui all'art.49, comma secondo Reg UE 2016/679, la documentazione delle garanzie adeguate	Sub Responsabili (Art. 21 comma 8 Reg Provinciale)	Incaricati trattamento (Art. 22 Reg Provinciale) (COGNOME E NOME)																																																																																			
	<table border="1"> <tr> <td>Adempimento di un obbligo legale al quale è soggetta la Provincia</td> <td></td> </tr> <tr> <td>Esecuzione di un contratto con riguardo ai soggetti interessati;</td> <td></td> </tr> <tr> <td>Per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.</td> <td></td> </tr> </table>	Adempimento di un obbligo legale al quale è soggetta la Provincia		Esecuzione di un contratto con riguardo ai soggetti interessati;		Per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.		<table border="1"> <tr><td>Raccolta</td><td></td></tr> <tr><td>Registrazione</td><td></td></tr> <tr><td>Organizzazione</td><td></td></tr> <tr><td>Conservazione</td><td></td></tr> <tr><td>Adattamento</td><td></td></tr> <tr><td>Modifica</td><td></td></tr> <tr><td>Estrazione</td><td></td></tr> <tr><td>Consultazione</td><td></td></tr> <tr><td>Uso</td><td></td></tr> </table> <table border="1"> <tr><td>Comunicazione mediante trasmissione</td><td></td></tr> <tr><td>Diffusione o qualsiasi altra forma di messa a disposizione</td><td></td></tr> </table> <table border="1"> <tr><td>Raffronto</td><td></td></tr> <tr><td>Interconnessione</td><td></td></tr> <tr><td>Limitazione</td><td></td></tr> <tr><td>Cancellazione</td><td></td></tr> <tr><td>Distruzione</td><td></td></tr> </table>	Raccolta		Registrazione		Organizzazione		Conservazione		Adattamento		Modifica		Estrazione		Consultazione		Uso		Comunicazione mediante trasmissione		Diffusione o qualsiasi altra forma di messa a disposizione		Raffronto		Interconnessione		Limitazione		Cancellazione		Distruzione		<table border="1"> <tr><td>Informatica</td><td></td></tr> <tr><td>Cartacea</td><td></td></tr> <tr><td>Mista</td><td></td></tr> <tr><td>Audio-visiva</td><td></td></tr> <tr><td>Fotografica</td><td></td></tr> <tr><td>Altro</td><td></td></tr> </table>	Informatica		Cartacea		Mista		Audio-visiva		Fotografica		Altro		<table border="1"> <tr><td>Utenti richiedenti il servizio</td><td></td></tr> <tr><td>Cittadini residenti nella provincia</td><td></td></tr> <tr><td>Chiunque</td><td></td></tr> <tr><td>Altro (specificare)</td><td></td></tr> </table>	Utenti richiedenti il servizio		Cittadini residenti nella provincia		Chiunque		Altro (specificare)		<table border="1"> <tr><td>Ordini professionali</td><td></td></tr> <tr><td>Enti di istruzione-Università privati</td><td></td></tr> <tr><td>Al richiedente l'accesso agli atti ove ne ricorrano i presupposti</td><td></td></tr> <tr><td>Altro (specificare)</td><td></td></tr> </table>	Ordini professionali		Enti di istruzione-Università privati		Al richiedente l'accesso agli atti ove ne ricorrano i presupposti		Altro (specificare)			<table border="1"> <tr><td>SI</td><td>NO</td></tr> </table> <table border="1"> <tr><td>In caso di risposta affermativa indicare COGNOME e NOME del Sub Responsabile</td><td></td></tr> <tr><td>- .</td><td></td></tr> <tr><td>- .</td><td></td></tr> <tr><td>- .</td><td></td></tr> <tr><td>- .</td><td></td></tr> <tr><td>- .</td><td></td></tr> <tr><td>- .</td><td></td></tr> <tr><td>- .</td><td></td></tr> </table>	SI	NO	In caso di risposta affermativa indicare COGNOME e NOME del Sub Responsabile		- .		- .		- .		- .		- .		- .		- .		
Adempimento di un obbligo legale al quale è soggetta la Provincia																																																																																												
Esecuzione di un contratto con riguardo ai soggetti interessati;																																																																																												
Per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.																																																																																												
Raccolta																																																																																												
Registrazione																																																																																												
Organizzazione																																																																																												
Conservazione																																																																																												
Adattamento																																																																																												
Modifica																																																																																												
Estrazione																																																																																												
Consultazione																																																																																												
Uso																																																																																												
Comunicazione mediante trasmissione																																																																																												
Diffusione o qualsiasi altra forma di messa a disposizione																																																																																												
Raffronto																																																																																												
Interconnessione																																																																																												
Limitazione																																																																																												
Cancellazione																																																																																												
Distruzione																																																																																												
Informatica																																																																																												
Cartacea																																																																																												
Mista																																																																																												
Audio-visiva																																																																																												
Fotografica																																																																																												
Altro																																																																																												
Utenti richiedenti il servizio																																																																																												
Cittadini residenti nella provincia																																																																																												
Chiunque																																																																																												
Altro (specificare)																																																																																												
Ordini professionali																																																																																												
Enti di istruzione-Università privati																																																																																												
Al richiedente l'accesso agli atti ove ne ricorrano i presupposti																																																																																												
Altro (specificare)																																																																																												
SI	NO																																																																																											
In caso di risposta affermativa indicare COGNOME e NOME del Sub Responsabile																																																																																												
- .																																																																																												
- .																																																																																												
- .																																																																																												
- .																																																																																												
- .																																																																																												
- .																																																																																												
- .																																																																																												

TABELLA B INFORMAZIONI SUI LUOGHI, STRUMENTI INFORMATICI E NON, SULLE MISURE E SUI RISCHI RELATIVI A TRATTAMENTI

SERVIZIO _____ UFFICIO _____

TRATTAMENTI

Codifica	Breve Descrizione	Codifica	Breve Descrizione
n.b.d		n.b.d	
n.b.d +1		n.b.d +4	
n.b.d +2		n.b.d +5	
n.b.d +3		n.b.d +6	

STRUMENTI ELETTRONICI		STRUMENTI NON INFORMATICI		RISCHI				MISURE - ELEMENTI DESCRITTIVI			DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE ORGANIZZATIVE DI CUI ALL'ART.32 PARAGRAFO 1 REG EU 2016/679																																																																																																																																																														
<table border="1"> <tr> <td rowspan="4">Tipologia</td> <td>Pc senza collegamento ad una rete dati e/o telefonica</td> <td></td> <td></td> </tr> <tr> <td>Pc connesso a sola rete interna o VPN</td> <td></td> <td></td> </tr> <tr> <td>Pc connesso a rete esterna</td> <td></td> <td></td> </tr> <tr> <td>Altro</td> <td></td> <td></td> </tr> </table>		Tipologia	Pc senza collegamento ad una rete dati e/o telefonica			Pc connesso a sola rete interna o VPN			Pc connesso a rete esterna			Altro			<table border="1"> <tr> <td>Armadio senza serratura</td> <td></td> </tr> <tr> <td>Armadio con serratura</td> <td></td> </tr> <tr> <td>Armadio ignifugo</td> <td></td> </tr> <tr> <td>Armadio semiblandato</td> <td></td> </tr> <tr> <td>Schedario</td> <td></td> </tr> <tr> <td>Cassaforte</td> <td></td> </tr> <tr> <td>Altro</td> <td></td> </tr> </table>		Armadio senza serratura		Armadio con serratura		Armadio ignifugo		Armadio semiblandato		Schedario		Cassaforte		Altro		<p>A RISCHI RELATIVI AI COMPORTAMENTI DEGLI OPERATORI e/o AL CONTESTO</p> <table border="1"> <thead> <tr> <th rowspan="2">Rischi</th> <th rowspan="2">Sussiste</th> <th colspan="3">Gravità impatto</th> </tr> <tr> <th>Bassa</th> <th>Media</th> <th>Alta</th> </tr> </thead> <tbody> <tr> <td rowspan="2">Sottrazione credenziali di autenticazione</td> <td>Si</td> <td>No</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td rowspan="2">Carenza di consapevolezza, disattenzione ed incuria</td> <td>Si</td> <td>No</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td rowspan="2">Comportamenti sleali o fraudolenti</td> <td>Si</td> <td>No</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td rowspan="2">Errore materiale</td> <td>Si</td> <td>No</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td rowspan="2">Altro</td> <td>Si</td> <td>No</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Rischi	Sussiste	Gravità impatto			Bassa	Media	Alta	Sottrazione credenziali di autenticazione	Si	No							Carenza di consapevolezza, disattenzione ed incuria	Si	No							Comportamenti sleali o fraudolenti	Si	No							Errore materiale	Si	No							Altro	Si	No							<table border="1"> <thead> <tr> <th>Descrizione sintetica</th> <th>Elementi descrittivi</th> <th>attuate</th> </tr> </thead> <tbody> <tr> <td>Impianto di allarme</td> <td>Gli spazi interessati alla misura sono dotati di impianto di allarme in grado di rilevare e segnalare l'eventuale intrusione di soggetti non autorizzati</td> <td>SI NO</td> </tr> <tr> <td>Sistema rilevazione incendio</td> <td>Gli spazi interessati alla misura sono dotati di impianto rilevazione incendi</td> <td>SI NO</td> </tr> <tr> <td>Inferrate o blindature alle vie di accesso</td> <td>La via di accesso agli spazi interessati alla misura è dotata di protezione fisica tipo inferrate o blindature in grado di impedire o comunque rendere difficile l'ingresso agli stessi senza la disponibilità delle relative chiavi</td> <td>SI NO</td> </tr> <tr> <td>Porte chiudibili a chiave</td> <td>L'accessibilità agli spazi interessati alla misura assoggettata all'utilizzazione di un'apposita chiave, disponibile solo per i soggetti appositamente autorizzati</td> <td>SI NO</td> </tr> <tr> <td>Armadi a pareti ignifughe</td> <td>Armadio di contenimento con pareti in grado di resistere al fuoco ed alle temperature per un tempo sufficiente a porre in sicurezza i contenuti dello stesso prima del loro deterioramento</td> <td>SI NO</td> </tr> <tr> <td>Estintori</td> <td>I locali sono dotati di appositi estintori</td> <td>SI NO</td> </tr> <tr> <td>Climatizzatore</td> <td>Il locale o vano oggetto della protezione è opportunamente climatizzato per poter assicurare il mantenimento di temperature operative compatibili durante tutto il periodo dell'anno</td> <td>SI NO</td> </tr> <tr> <td>Armadi e cassetiere chiudibili a chiave</td> <td>Gli armadi e cassetiere interessati alla misura sono assoggettati all'utilizzazione di apposita chiave disponibile solo per i soggetti appositamente autorizzati</td> <td>SI NO</td> </tr> <tr> <td>Gruppo statico di continuità (UPS)</td> <td>Il carico elettrico da proteggere è alimentato attraverso un gruppo statico di continuità in grado di erogare, senza interruzione, la potenza elettrica necessaria per un tempo sufficiente a porre in sicurezza il carico stesso</td> <td>SI NO</td> </tr> <tr> <td>Linea elettrica dedicata</td> <td>Al fine di eliminare interruzioni al carico da proteggere derivanti da problemi relativi ad alti carichi. Questo viene alimentato con linea elettrica separata e dedicata dal quadro generale più vicino.</td> <td>SI NO</td> </tr> <tr> <td>Password condivisa di accesso alla stazione</td> <td>L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso</td> <td>SI NO</td> </tr> <tr> <td>Password personale di accesso alla stazione</td> <td>L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto solo dalla persona</td> <td>SI NO</td> </tr> </tbody> </table>			Descrizione sintetica	Elementi descrittivi	attuate	Impianto di allarme	Gli spazi interessati alla misura sono dotati di impianto di allarme in grado di rilevare e segnalare l'eventuale intrusione di soggetti non autorizzati	SI NO	Sistema rilevazione incendio	Gli spazi interessati alla misura sono dotati di impianto rilevazione incendi	SI NO	Inferrate o blindature alle vie di accesso	La via di accesso agli spazi interessati alla misura è dotata di protezione fisica tipo inferrate o blindature in grado di impedire o comunque rendere difficile l'ingresso agli stessi senza la disponibilità delle relative chiavi	SI NO	Porte chiudibili a chiave	L'accessibilità agli spazi interessati alla misura assoggettata all'utilizzazione di un'apposita chiave, disponibile solo per i soggetti appositamente autorizzati	SI NO	Armadi a pareti ignifughe	Armadio di contenimento con pareti in grado di resistere al fuoco ed alle temperature per un tempo sufficiente a porre in sicurezza i contenuti dello stesso prima del loro deterioramento	SI NO	Estintori	I locali sono dotati di appositi estintori	SI NO	Climatizzatore	Il locale o vano oggetto della protezione è opportunamente climatizzato per poter assicurare il mantenimento di temperature operative compatibili durante tutto il periodo dell'anno	SI NO	Armadi e cassetiere chiudibili a chiave	Gli armadi e cassetiere interessati alla misura sono assoggettati all'utilizzazione di apposita chiave disponibile solo per i soggetti appositamente autorizzati	SI NO	Gruppo statico di continuità (UPS)	Il carico elettrico da proteggere è alimentato attraverso un gruppo statico di continuità in grado di erogare, senza interruzione, la potenza elettrica necessaria per un tempo sufficiente a porre in sicurezza il carico stesso	SI NO	Linea elettrica dedicata	Al fine di eliminare interruzioni al carico da proteggere derivanti da problemi relativi ad alti carichi. Questo viene alimentato con linea elettrica separata e dedicata dal quadro generale più vicino.	SI NO	Password condivisa di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso	SI NO	Password personale di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto solo dalla persona	SI NO	<table border="1"> <tbody> <tr> <td>Pseudonimizzazione</td> <td>SI NO</td> <td>Sistemi di protezione con videosorveglianza</td> <td>SI NO</td> </tr> <tr> <td>Minimizzazione</td> <td>SI NO</td> <td>Registrazione di accessi</td> <td>SI NO</td> </tr> <tr> <td>Cifatura dei dati personali</td> <td>SI NO</td> <td>Porte, armadi e contenitori dotati di serrature ed ignifughi</td> <td>SI NO</td> </tr> <tr> <td>Capacità di assicurare la continua riservatezza</td> <td>SI NO</td> <td>Sistemi di copiatura e conservazione di archivi elettronici</td> <td>SI NO</td> </tr> <tr> <td>Integrità</td> <td>SI NO</td> <td>Misure antincendio</td> <td>SI NO</td> </tr> <tr> <td>Disponibilità e resistenza dei sistemi cui sono trattati i dati personali</td> <td>SI NO</td> <td>Sistemi di rilevazione di intrusione</td> <td>SI NO</td> </tr> <tr> <td>Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico</td> <td>SI NO</td> <td>Sistemi di sorveglianza</td> <td>SI NO</td> </tr> <tr> <td>Procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative, al fine di garantire la sicurezza del trattamento</td> <td>SI NO</td> <td>Altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico</td> <td>SI NO</td> </tr> <tr> <td>Sistemi di autenticazione, autorizzazione protezione (antivirus, firewall, antintrusione, altro)</td> <td>SI NO</td> <td></td> <td></td> </tr> </tbody> </table>				Pseudonimizzazione	SI NO	Sistemi di protezione con videosorveglianza	SI NO	Minimizzazione	SI NO	Registrazione di accessi	SI NO	Cifatura dei dati personali	SI NO	Porte, armadi e contenitori dotati di serrature ed ignifughi	SI NO	Capacità di assicurare la continua riservatezza	SI NO	Sistemi di copiatura e conservazione di archivi elettronici	SI NO	Integrità	SI NO	Misure antincendio	SI NO	Disponibilità e resistenza dei sistemi cui sono trattati i dati personali	SI NO	Sistemi di rilevazione di intrusione	SI NO	Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico	SI NO	Sistemi di sorveglianza	SI NO	Procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative, al fine di garantire la sicurezza del trattamento	SI NO	Altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico	SI NO	Sistemi di autenticazione, autorizzazione protezione (antivirus, firewall, antintrusione, altro)	SI NO		
Tipologia	Pc senza collegamento ad una rete dati e/o telefonica																																																																																																																																																																								
	Pc connesso a sola rete interna o VPN																																																																																																																																																																								
	Pc connesso a rete esterna																																																																																																																																																																								
	Altro																																																																																																																																																																								
Armadio senza serratura																																																																																																																																																																									
Armadio con serratura																																																																																																																																																																									
Armadio ignifugo																																																																																																																																																																									
Armadio semiblandato																																																																																																																																																																									
Schedario																																																																																																																																																																									
Cassaforte																																																																																																																																																																									
Altro																																																																																																																																																																									
Rischi	Sussiste	Gravità impatto																																																																																																																																																																							
		Bassa	Media	Alta																																																																																																																																																																					
Sottrazione credenziali di autenticazione	Si	No																																																																																																																																																																							
Carenza di consapevolezza, disattenzione ed incuria	Si	No																																																																																																																																																																							
Comportamenti sleali o fraudolenti	Si	No																																																																																																																																																																							
Errore materiale	Si	No																																																																																																																																																																							
Altro	Si	No																																																																																																																																																																							
Descrizione sintetica	Elementi descrittivi	attuate																																																																																																																																																																							
Impianto di allarme	Gli spazi interessati alla misura sono dotati di impianto di allarme in grado di rilevare e segnalare l'eventuale intrusione di soggetti non autorizzati	SI NO																																																																																																																																																																							
Sistema rilevazione incendio	Gli spazi interessati alla misura sono dotati di impianto rilevazione incendi	SI NO																																																																																																																																																																							
Inferrate o blindature alle vie di accesso	La via di accesso agli spazi interessati alla misura è dotata di protezione fisica tipo inferrate o blindature in grado di impedire o comunque rendere difficile l'ingresso agli stessi senza la disponibilità delle relative chiavi	SI NO																																																																																																																																																																							
Porte chiudibili a chiave	L'accessibilità agli spazi interessati alla misura assoggettata all'utilizzazione di un'apposita chiave, disponibile solo per i soggetti appositamente autorizzati	SI NO																																																																																																																																																																							
Armadi a pareti ignifughe	Armadio di contenimento con pareti in grado di resistere al fuoco ed alle temperature per un tempo sufficiente a porre in sicurezza i contenuti dello stesso prima del loro deterioramento	SI NO																																																																																																																																																																							
Estintori	I locali sono dotati di appositi estintori	SI NO																																																																																																																																																																							
Climatizzatore	Il locale o vano oggetto della protezione è opportunamente climatizzato per poter assicurare il mantenimento di temperature operative compatibili durante tutto il periodo dell'anno	SI NO																																																																																																																																																																							
Armadi e cassetiere chiudibili a chiave	Gli armadi e cassetiere interessati alla misura sono assoggettati all'utilizzazione di apposita chiave disponibile solo per i soggetti appositamente autorizzati	SI NO																																																																																																																																																																							
Gruppo statico di continuità (UPS)	Il carico elettrico da proteggere è alimentato attraverso un gruppo statico di continuità in grado di erogare, senza interruzione, la potenza elettrica necessaria per un tempo sufficiente a porre in sicurezza il carico stesso	SI NO																																																																																																																																																																							
Linea elettrica dedicata	Al fine di eliminare interruzioni al carico da proteggere derivanti da problemi relativi ad alti carichi. Questo viene alimentato con linea elettrica separata e dedicata dal quadro generale più vicino.	SI NO																																																																																																																																																																							
Password condivisa di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso	SI NO																																																																																																																																																																							
Password personale di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto solo dalla persona	SI NO																																																																																																																																																																							
Pseudonimizzazione	SI NO	Sistemi di protezione con videosorveglianza	SI NO																																																																																																																																																																						
Minimizzazione	SI NO	Registrazione di accessi	SI NO																																																																																																																																																																						
Cifatura dei dati personali	SI NO	Porte, armadi e contenitori dotati di serrature ed ignifughi	SI NO																																																																																																																																																																						
Capacità di assicurare la continua riservatezza	SI NO	Sistemi di copiatura e conservazione di archivi elettronici	SI NO																																																																																																																																																																						
Integrità	SI NO	Misure antincendio	SI NO																																																																																																																																																																						
Disponibilità e resistenza dei sistemi cui sono trattati i dati personali	SI NO	Sistemi di rilevazione di intrusione	SI NO																																																																																																																																																																						
Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico	SI NO	Sistemi di sorveglianza	SI NO																																																																																																																																																																						
Procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative, al fine di garantire la sicurezza del trattamento	SI NO	Altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico	SI NO																																																																																																																																																																						
Sistemi di autenticazione, autorizzazione protezione (antivirus, firewall, antintrusione, altro)	SI NO																																																																																																																																																																								
<table border="1"> <tr> <td>Interconnessione</td> <td></td> <td></td> </tr> </table>		Interconnessione			<table border="1"> <tr> <td>Si</td> <td>No</td> </tr> </table>		Si	No	<p>B RISCHI RELATIVI AGLI STRUMENTI</p> <table border="1"> <thead> <tr> <th rowspan="2">Rischi</th> <th rowspan="2">Sussiste</th> <th colspan="3">Gravità impatto</th> </tr> <tr> <th>Bassa</th> <th>Media</th> <th>Alta</th> </tr> </thead> <tbody> <tr> <td rowspan="2">Azioni di virus informatici o programmi suscettibili di recare danno</td> <td>Si</td> <td>No</td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Rischi	Sussiste	Gravità impatto			Bassa	Media	Alta	Azioni di virus informatici o programmi suscettibili di recare danno	Si	No							<table border="1"> <thead> <tr> <th>Descrizione sintetica</th> <th>Elementi descrittivi</th> <th>attuate</th> </tr> </thead> <tbody> <tr> <td>Password condivisa di accesso alla stazione</td> <td>L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso</td> <td>SI NO</td> </tr> <tr> <td>Password personale di accesso alla stazione</td> <td>L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto solo dalla persona</td> <td>SI NO</td> </tr> </tbody> </table>			Descrizione sintetica	Elementi descrittivi	attuate	Password condivisa di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso	SI NO	Password personale di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto solo dalla persona	SI NO																																																																																																																																
Interconnessione																																																																																																																																																																									
Si	No																																																																																																																																																																								
Rischi	Sussiste	Gravità impatto																																																																																																																																																																							
		Bassa	Media	Alta																																																																																																																																																																					
Azioni di virus informatici o programmi suscettibili di recare danno	Si	No																																																																																																																																																																							
Descrizione sintetica	Elementi descrittivi	attuate																																																																																																																																																																							
Password condivisa di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso	SI NO																																																																																																																																																																							
Password personale di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto solo dalla persona	SI NO																																																																																																																																																																							

				ta									
						Si No							
Spamming o tecniche di sabotaggio	Si No	Ba ss a	M ed ia	Al ta						Password condivisa di accesso alla stazione	L'accesso alla procedura informatica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso	SI	NO
										Sistema di autorizzazione e basato su profili	Il modulo software utilizzato per il trattamento dei dati oggetto della misura di protezione è basato su un sistema di profilazione dell'utenza che prevede di differenziare le possibili operazioni di trattamento eseguibili dai vari utenti in base al profilo/i specifico/i ad essi assegnati	SI	NO
Malfunzionamento, indisponibilità o degrado degli strumenti	Si No	Ba ss a	M ed ia	Al ta						Logging	L'accesso alla risorsa informatica in questione è assoggettato a tracciate delle operazioni effettuate con le registrazioni di: Epoca dell'operazione Indirizzo di rete della stazione accedente(se definito) Descrizione dell'operazione fatta-identificativo dell'utente che compie l'operazione. Tali file di log sono accuratamente conservati, per un tempo prestabilito per l'eventuale loro controllo.	SI	NO
										Accessi esterni non autorizzati	I dati programmi sono copiati con regolarità su supporti fisici diversi che sono poi conservati in locali separati opportunamente protetti da accessi non autorizzati	SI	NO
Intercettazioni e di informazioni in rete	Si No	Ba ss a	M ed ia	Al ta						Backup	Le procedure di backup sono effettuate producendo copie multiple che sono poi conservate in locali diversi ciascuno soggetti ad opportune restrizioni di accesso	SI	NO
										Copie multiple	Il supporto fisico contenente i dati in questione che non risultano più necessari e quindi oggetto di protezione, viene cancellato mediante le opportune tecniche dipendenti dalla natura del supporto stesso. Tali operazioni di cancellazione renderanno il contenuto di tale supporto non più leggibile con strumenti informatici di normale uso	SI	NO
Altro	Si No	Ba ss a	M ed ia	Al ta						Cancellazione dei supporti fisici contenenti dati non più necessari	Gli incaricati del trattamento sulla banca oggetto della misura sono stati resi edotti, in modo specifico e puntuale, degli eventi dannosi relativi a quella banca dati e sulle misure adottate per contrastare il rischio derivante. Sono state poi date istruzioni operative dettagliate sul come rendere operative le misure di contrasto del rischio	SI	NO
										Informazione/formazione specifica sul rischio	Sui sistemi interessati al trattamento dei dati in questione sono stati installati opportuni software di protezione dai virus informatici. Tali software sono costantemente aggiornati, in modo automatico, con frequenza almeno giornaliera.	SI	NO
										Modifica periodica delle credenziali	Le credenziali di accesso, quali password o certificati digitali, vengono rinnovate con una frequenza idonea a garantire le banche dati accedute da utilizzo delle stesse da parte di soggetti non autorizzati che abbiano sottratto o generato, con opportune procedure di password cracking, le stesse.	SI	NO
										Password dello screen saver	Quando la postazione di lavoro è lasciata incustodita, si avvia in automatico dopo un intervallo di tempo, lo screen saver. La disattivazione dello screen saver richiede l'inserimento di una password	SI	NO

Il Responsabile del trattamento

Il/I Sub responsabile/i del trattamento
