PROVINCIA AUTONOMA DI TRENTO

Reg. delib. n. 54 Prot. n.

VERBALE DI DELIBERAZIONE DELLA GIUNTA PROVINCIALE

OGGETTO:
Regolamento UE 2016/679 e D. Lgs. 196/2003 aggiornato. Approvazione della policy in materia di privacy e misure di sicurezza informatica della Provincia e della principale modulistica in uso.

Il giorno **25 Gennaio 2019** ad ore **09:35** nella sala delle Sedute
in seguito a convocazione disposta con avviso agli assessori, si è riunita

LA GIUNTA PROVINCIALE

sotto la presidenza del

	PRESIDENTE	**MAURIZIO FUGATTI**
Presenti:	VICEPRESIDENTE	**MARIO TONINA**
	ASSESSORE	**ROBERTO FAILONI**
		STEFANIA SEGNANA
		ACHILLE SPINELLI
		GIULIA ZANOTELLI
Assenti:	ASSESSORE	**MIRKO BISESTI**
Assiste:	IL DIRIGENTE	**ENRICO MENAPACE**

Il Presidente, constatato il numero legale degli intervenuti, dichiara aperta la seduta

Il Relatore comunica:

in tema di protezione dei dati personali è entrato in vigore (24 maggio 2016) il Regolamento, del Parlamento europeo e del Consiglio, 2016/679 "*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*" (regolamento generale sulla protezione dei dati);

il provvedimento normativo dell'Unione europea è diventato vincolante, in ogni Stato membro, dal 25 maggio 2018 e prevede varie novità funzionali ed organizzative (valutazione d'impatto, *data breach*, formazione obbligatoria, Registro dei trattamenti, Responsabile della protezione dei dati, ecc.) di notevole rilevanza;

con legge n. 163/2017, il Parlamento ha delegato il Governo ad adattare il D. Lgs. n. 196/2003 (c.d. Codice privacy) al Regolamento UE 2016/679, nonché ad apportare, al provvedimento nazionale, le modifiche ritenute necessarie; il processo normativo di armonizzazione e di modifica/integrazione del Codice privacy si è concluso con l'adozione del D. Lgs. n. 101 del 10 agosto 2018, entrato in vigore in data 19 settembre 2018;

per realizzare un'efficace politica di protezione dati personali, la quale, particolare non trascurabile, esplica "direttamente" i propri effetti su tutte le funzioni ed i procedimenti amministrativi di ogni soggetto pubblico/Titolare del trattamento, è quindi necessario ottemperare, nei modi e nei tempi stabiliti, agli obblighi previsti dalla normativa europea e nazionale attraverso la predisposizione di un apposito modello organizzativo e procedurale;

ritenuto come tale modello debba coniugare una precisa e chiara rappresentazione dei processi e dei principi normativi vigenti, con la finalità di semplificazione dell'attività amministrativa;

con il presente provvedimento, dunque, si intende dotare i vari soggetti–(Dirigenti, Direttori, Dipendenti, Responsabili esterni del trattamento, collaboratori esterni, ecc.), che trattano, anche in via incidentale, dati personali per conto della Provincia, di uno strumento che contenga adeguate istruzioni e procedure per la gestione degli stessi;

constatato che il D. Lgs. n. 196/2003 (art. 2-*quaterdecies*) autorizza il Titolare ad assegnare "*specifici compiti e funzioni connessi al trattamento di dati personali*" a persone fisiche che agiscono sotto la propria diretta autorità;

ritenuto opportuno per la gestione dei trattamenti di dati personali, anche tenuto conto della complessità organizzativa della Provincia, nonché della molteplicità ed eterogeneità delle funzioni alla stessa attribuite, denominare i Dirigenti della Provincia Preposti al trattamento, e le persone fisiche, assegnate alle strutture dai medesimi dirette, Addetti al trattamento;

appurata la necessità che il Titolare del trattamento autorizzi il Dirigente/Preposto al trattamento a determinare, con proprio provvedimento e previa intesa con la Struttura competente in materia di sicurezza informatica, ulteriori misure di sicurezza, in aggiunta a quelle generali e *standard*, potendo lo stesso essere in possesso di una cognizione specifica e diretta dei rischi connessi alla gestione dei dati personali;

ritenuto indispensabile, per l'effettiva realizzazione di un efficiente modello di gestione dei trattamenti dei dati, designare, in seno alle varie Strutture provinciali, una figura che, anche fungendo da collegamento con la Struttura specificamente competente in materia di dati personali, dedichi parte del proprio tempo alla cura e attuazione degli adempimenti in materia di protezione dei dati;

Tutto ciò premesso,

LA GIUNTA PROVINCIALE

- visto il Regolamento, del Parlamento europeo e del Consiglio, 2016/679;
- visto il D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), così come novellato dal D. Lgs. n. 101/2018;
- viste le deliberazioni della Giunta provinciale nn. 2643/2008, 1037/2010, 2081/2016, 450/2018 e 2004/2018;

a voti unanimi, espressi nelle forme di legge;

d e l i b e r a

1) di approvare, per le ragioni in premessa illustrate, in conformità a quanto disposto dal Regolamento UE 2016/679 e dal D. Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) le policy sulla protezione dei dati personali contenute negli Allegati: A) Principali prescrizioni; B) Privacy & Digital policy della Provincia autonoma di Trento; che costituiscono parte integrante e sostanziale del presente provvedimento, demandando ai Dirigenti/Preposti al trattamento la cura degli adempimenti previsti nei richiamati allegati;
2) di revocare la deliberazione della Giunta provinciale n. 1081/2013, sostituita dal presente provvedimento;
3) di inviare la presente deliberazione, per gli adempimenti di rispettiva competenza, a tutte le Strutture provinciali, nonché a Trentino Digitale S.p.a.;
4) di disporre la pubblicazione del presente provvedimento sul sito istituzionale della Provincia autonoma di Trento.

Adunanza chiusa ad ore 11:00

Verbale letto, approvato e sottoscritto.

Elenco degli allegati parte integrante

001 Allegato A

002 Allegato B

IL PRESIDENTE
Maurizio Fugatti

IL DIRIGENTE
Enrico Menapace

ALLEGATO A

PRINCIPALI PRESCRIZIONI DELLA DELIBERAZIONE

1) La Provincia autonoma di Trento è Titolare dei trattamenti dei dati personali finalizzati all'esercizio delle funzioni istituzionali attribuite dall'ordinamento; il Titolare del trattamento, nell'attuazione della normativa, agisce tramite il Presidente e la Giunta provinciale.

2) Ai sensi dell'art. 2-*quaterdecies* del D. Lgs. n. 196/2003, i Dirigenti della Provincia, relativamente ai trattamenti riconducibili alla loro competenza, sono qualificati come Preposti al trattamento, mentre le restanti persone fisiche che agiscono sotto l'autorità del Titolare sono denominate Addetti al trattamento; gli stessi sono tenuti a rispettare le istruzioni loro impartite e contenute nella presente deliberazione.

3) La Società Informatica Trentina s.p.a. (oggi Trentino Digitale S.p.a.) è stata nominata Responsabile dei trattamenti della Provincia, affidati alla Società stessa ai sensi della legge provinciale n. 16/2012, nell'ambito delle prestazioni definite dalla Convenzione sottoscritta dalle parti in data 24 maggio 2013.

4) Trentino Digitale S.p.a., quale Responsabile esterno del trattamento dei dati personali della Provincia autonoma di Trento, è tenuta ad adottare tutte le misure idonee a garantire un livello di sicurezza adeguato ai rischi, nonché a predisporre ed aggiornare l'analisi dei rischi, correlati agli strumenti informatici gestiti dalla Società e messi a disposizione del Titolare, nonché la metodologia della valutazione di impatto.

5) Ai Dirigenti/Preposti è demandato il compito di stipulare, con i soggetti esterni che collaborano con la Provincia per l'esercizio delle funzioni istituzionali, il contratto per la gestione dei trattamenti di dati personali. I collaboratori esterni sono nominati, dal Dirigente/Preposto, Responsabili esterni del trattamento solo dopo aver individuato il ruolo ritenuto più idoneo, posto che gli stessi soggetti potrebbero anche essere qualificati, in alternativa, come Titolari autonomi, o Contitolari del trattamento (ovvero ancora, Autorizzati al trattamento). Ad integrazione delle attribuzioni in tema di qualificazione dei Responsabili esterni, i Dirigenti/Preposti impartiscono, inoltre, ai medesimi le istruzioni connesse all'assunzione del predetto ruolo.

6) Spetta ai Dirigenti/Preposti autorizzare al trattamento gli Addetti, definendone l'ambito del trattamento consentito; nello svolgimento di tale attività i Preposti potranno fare riferimento a tutte le informazioni contenute nel Registro dei trattamenti provinciali. I Dirigenti/Preposti al trattamento sono tenuti ad inserire, nel Registro dei trattamenti, i nominativi degli Addetti, associandoli ai trattamenti di loro pertinenza. Gli Addetti possono trattare, solo ed esclusivamente, i dati di loro competenza; nel caso di trasferimento, anche temporaneo, ad altra Struttura/Ufficio, l'Addetto perde i privilegi di accesso ai dati personali rientranti nella competenza dell'ufficio di provenienza, salvo l'ipotesi di contestuale assegnazione a più Strutture o, a più compiti, relativi a Strutture diverse.

7) Agli Addetti sono impartite le istruzioni generali, indicate nella presente deliberazione, che definiscono l'ambito del trattamento consentito. Il contenuto delle istruzioni dovrà essere, ad opera dei Dirigenti/ Preposti, integrato e costantemente aggiornato, anche con eventuali e più specifiche prescrizioni, qualora lo richiedano la peculiarità dei trattamenti ed il contesto nel quale gli stessi si svolgono.

8) I Dirigenti/Preposti individuano, nell'ambito delle Strutture di rispettiva competenza ed utilizzando i criteri e le modalità stabiliti nella presente deliberazione, collaboratori (c.d. Referenti privacy) che si occupano, congiuntamente alle proprie mansioni, anche della cura e attuazione delle disposizioni in materia di protezione dei dati personali, i quali sono tenuti a coordinarsi con la Struttura provinciale competente in materia di protezione dei dati personali.

9) I Dirigenti/Preposti provvedono, nell'ambito delle Strutture di appartenenza, alla nomina degli Amministratori di sistema degli eventuali sistemi informativi non gestiti da Trentino Digitale S.p.a.. I Dirigenti/Preposti al trattamento, inoltre, dovranno inserire i nominativi degli Amministratori di sistema, nonché l'ambito di operatività e le funzioni attribuite ai medesimi, nel Registro dei trattamenti provinciali, garantendo il costante aggiornamento di tali informazioni. Trentino Digitale S.p.a., a propria volta, è tenuta a nominare, ai sensi del contratto stipulato con la Provincia autonoma di Trento, gli Amministratori di sistema, della società, che operano sui trattamenti della Provincia autonoma.

10) I Dirigenti/Preposti sono incaricati di vigilare sull'osservanza delle misure di sicurezza e sulle istruzioni adottate dal Titolare. Le Struttura provinciale competente in materia di sicurezza informatica è incaricata, ove ritenuto necessario avvalendosi di soggetti esterni, di svolgere i controlli in materia.

11) La Struttura provinciale competente in materia di sicurezza informatica può individuare, ove lo ritenga necessario, ulteriori istruzioni attuative (ad integrazione, specificazione e chiarimento) delle disposizioni precisate nella Sezione II, dell'Allegato B, della presente deliberazione o delle eventuali ulteriori disposizioni della Giunta provinciale.

12) I Dirigenti/Preposti al trattamento sono tenuti ad effettuare il censimento dei trattamenti dei dati personali in atto e delle banche dati in uso nell'ambito delle Strutture di competenza, inserendo tali informazioni nel Registro elettronico dei trattamenti, reperibile all'indirizzo http://trattamenti.provincia.tn.it.

13) Il contenuto della modulistica, allegata alla presente deliberazione, costituisce il livello minimo per il puntuale adempimento degli obblighi previsti dal Regolamento UE 2016/679. I Dirigenti/Preposti al trattamento, in ogni caso, sono autorizzati ad apportare – integrando/variando il contenuto dei modelli – le modifiche ritenute necessarie e/o opportune ai fini dell'adeguamento, degli stessi, alle specifiche peculiarità dei trattamenti di competenza delle Strutture delle quali sono responsabili, fermi gli obblighi di legge.

ALLEGATO B

PRIVACY & DIGITAL POLICY

DELLA PROVINCIA AUTONOMA DI TRENTO

ai sensi del Regolamento, del Parlamento europeo e del Consiglio, 2016/679 "*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 (regolamento generale sulla protezione dei dati)*" e del D. Lgs. n. 196/2003 (così come armonizzato dal D. Lgs. n. 101/2018).

INDICE

INTRODUZIONE

Il diritto alla protezione dei dati personali è particolarmente rilevante nell'ambito dell'attività amministrativa e richiede un bilanciamento tra la necessità degli enti pubblici di acquisire e trattare dati personali, strumentali all'attuazione dei compiti istituzionali, e l'interesse dei cittadini all'efficienza dell'Amministrazione e alla tutela dei propri dati. D'altra parte, non può tacersi il fatto che lo sviluppo tecnologico e l'evoluzione delle reti telematiche espongano il singolo individuo ad un rischio di abuso, anche inconsapevole, della sfera privata e delle informazioni che lo riguardano.
Per fronteggiare la situazione sopra descritta, il legislatore europeo aveva emanato la Direttiva 95/46/CE, a sua volta recepita, nell'ordinamento nazionale, dal Decreto Legislativo 30 giugno 2003, n. 196, contenente il "Codice in materia di protezione dei dati personali" (di seguito, anche definito il "Codice"); l'attuale legislatore dell'Unione europea, per contrastare l'eccessiva diversificazione delle disposizioni nazionali in tema di protezione dati, adottate dai vari Stati membri, ha recentemente emanato un nuovo strumento normativo, ovvero il Regolamento, del Parlamento europeo e del Consiglio, 2016/679 "*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*, (regolamento generale sulla protezione dei dati)" allo specifico fine di uniformare, in tutto il territorio dell'Unione, la disciplina della tutela dei dati personali. Con D. Lgs. n. 101/2018, che ha altresì apportato revisioni alle disposizioni concernenti le sanzioni amministrative e penali, il D. Lgs. n. 196/2003 è stato armonizzato con la richiamata normativa europea.

La tutela dei dati personali non può prescindere, inoltre, da un adeguato sistema di misure di sicurezza, in particolare quelle di natura informatica, considerato come ogni dato personale, anche se conservato come documento cartaceo, venga quasi sempre preventivamente trattato con apparecchiature elettroniche. L'odierno assetto normativo, inoltre, basato sul concetto di *accountability*, implica la capacità del Titolare (e, talvolta, del Responsabile esterno) di fornire adeguata prova del rispetto di ogni principio di legittimità di cui all'art. 5 del Regolamento UE 2016/679, nonché dei relativi obblighi di esecuzione (vedasi, ad esempio, la consegna dell'informativa). Permane, poi, una concezione del trattamento quale attività pericolosa, con la conseguente attribuzione di una responsabilità oggettiva in capo al Titolare: ciò implica che al danneggiato è sufficiente fornire esclusivamente prova del danno subito e del nesso eziologico (cioè, di causalità tra evento e danno stesso), gravando sul Titolare (secondo il principio dell'inversione dell'onere probatorio) la prova di aver adottato tutte le cautele idonee ad evitare il danno.

La Provincia autonoma di Trento, nella veste di Titolare del trattamento, attraverso una serie di regole di attuazione del citato Regolamento UE 2016/679, ha predisposto il presente provvedimento per favorire l'uniforme applicazione della normativa in materia di protezione dei dati personali, anche mediante la disciplina dei singoli processi decisionali ed organizzativi. Pertanto, la deliberazione in oggetto rappresenta uno strumento operativo, a disposizione dei vari soggetti che assumono, nell'ambito dell'attività di gestione dei dati personali, i diversi ruoli previsti dalla normativa vigente; in particolare, l'obiettivo è quello di fornire, ai dipendenti, istruzioni in ordine alle varie misure (organizzative, procedurali, tecniche e logistiche) finalizzate a garantire il necessario livello di sicurezza dei trattamenti gestiti dall'Amministrazione provinciale. Tramite la codificazione dei compiti e degli adempimenti richiesti, i vari soggetti coinvolti nella gestione dei dati personali, compresi i collaboratori esterni dell'Amministrazione provinciale, saranno consapevoli dell'estensione dei compiti ad essi assegnati.

Il provvedimento si articola in tre sezioni (talvolta, divise in capitoli, paragrafi e sottoparagrafi):

- Sezione I: illustra le finalità e i principi generali che contraddistinguono il trattamento dei dati personali da parte dei soggetti pubblici;
- Sezione II: dedicata all'individuazione delle misure di sicurezza tecnico-informatiche, che i vari soggetti dell'Amministrazione provinciale sono tenuti a rispettare;
- Sezione III: contiene la modulistica adottata dal Titolare del trattamento.

Le Sezioni I e III sono state elaborate dal Direttore dell'Ufficio Organizzazione e gestione della privacy, con la consulenza del Responsabile della protezione dei dati. Si evidenzia che, per ragioni di sistematicità e comodità di lettura, il testo coordina le disposizioni normative più rilevanti per i soggetti pubblici, anche mediante sintesi e parafrasi delle disposizioni stesse; per tali ragioni, le Strutture sono tenute alla lettura integrale delle norme in vigore.
La Sezione II è stata elaborata dalle Strutture competenti in materia ICT e trasformazione digitale.
Per facilitarne la reperibilità nei confronti degli interessati, il testo del presente documento è disponibile in *internet* ("Protezione dati personali") alla sezione Amministrazione trasparente.

SEZIONE I
CONTESTO NORMATIVO

1. ATTI DELLA PROVINCIA AUTONOMA DI TRENTO IN TEMA DI TRATTAMENTO DEI DATI PERSONALI

I ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 17 OTTOBRE 2008, N. 2643***
(Procedure operative di sicurezza delle informazioni attuate dalle Strutture organizzative dipendenti dalla Giunta provinciale: approvazione del documento *"Procedura operativa per la gestione dei dispositivi di videosorveglianza*")

II ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 7 MAGGIO 2010, N. 1037***
(Utilizzo della rete *Internet*, della posta elettronica, delle attrezzature informatiche e telefoniche – Approvazione disciplinare)

III ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 24 NOVEMBRE 2016, N. 2081*** (Disciplinare della Provincia autonoma di Trento in tema di Amministratori di sistema)

IV ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 23 MARZO 2018, N. 450***
(Adozione, ai sensi dell'art. 30 del Regolamento UE n. 679/2016, del registro in formato elettronico delle attività di trattamento dei dati personali della Provincia autonoma di Trento e approvazione, ai sensi dell'art. 35 del medesimo Regolamento UE, della metodologia per la valutazione d'impatto dei trattamenti)

V ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 19 OTTOBRE 2018, N. 2004***
(Approvazione degli schemi di contratto di nomina del responsabile esterno del trattamento e modifica della metodologia per la valutazione d'impatto dei trattamenti di cui alla deliberazione della Giunta provinciale n. 450 del 23 marzo 2018)

I testi delle deliberazioni e le principali circolari, nonché la normativa in materia di protezione dei dati personali, sono disponibili nella *intranet* provinciale ("Privacy e sicurezza").

2. NOZIONI GENERALI E DEFINIZIONI

2.1 Finalità del Regolamento UE 2016/679

Il Regolamento UE 2016/679 (di seguito, anche definito "Regolamento"), finalizzato alla protezione dei diritti e libertà fondamentali delle persone fisiche, tutela, in particolare, il diritto alla protezione dei dati personali.

Il considerando n. 1 del Regolamento UE 2016/679 specifica che "***La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale***. *L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*", mentre il considerando n. 2 precisa che "***I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale ("dati personali") dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza***. *Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche*".

2.2 Glossario

2.2.1 Glossario *ex* art. 4, Regolamento UE 2016/679

«**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*;

«**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*;

«**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*;

«**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*;

«**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;

«**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*;

«**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*;

«**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*;

«**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*;

«**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*;

«**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*;

«**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*;

«**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*;

«**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*.

2.2.2 Glossario *ex* art. 2-*ter*, comma 4, D. Lgs. n. 196/2003

«**Comunicazione**»: *il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;*

«**Diffusione**»: *il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.*

2.3 Particolari categorie di dati (*ex* art. 9 del Regolamento UE 2016/679)

Appartengono a "particolari categorie" i dati personali che rivelano "*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale*", nonché i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

La definizione, che richiama, ampliandolo, il concetto di dato sensibile definito nella previgente versione del D. Lgs. n. 196/2003, è tassativa: sono considerati "particolari" solo i dati specificamente indicati nell'apposita norma, indipendentemente dal carattere di riservatezza o di particolare rilevanza che un individuo, o il senso comune, possano attribuire ad altre tipologie di dati (ad esempio: codice identificativo della carta di credito, reddito, stato di separazione, coordinate bancarie, ecc.).

2.4 Dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (*ex* art. 10 del Regolamento UE 2016/679)

L'articolo in esame prevede che il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (*ex* "dati giudiziari") è ammesso soltanto sotto il controllo dell'autorità pubblica o se autorizzato dal diritto dell'Unione o degli Stati membri.

2.5 Presupposti di liceità del trattamento dei dati personali da parte della Pubblica Amministrazione

L'articolo 5.1 del Regolamento UE 2016/679 (Principi applicabili al trattamento di dati personali) definisce le regole entro le quali deve svolgersi il trattamento, specificando che: "*I dati personali sono:*
*a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);*
*b) 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'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («**limitazione della finalità**»);*
*c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);*
*d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);*
*e) 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'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);*
*f) 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 («**integrità e riservatezza**»)*".

L'articolo 6.1 del Regolamento UE 2016/679 recita: "***il trattamento è lecito solo se*** *ricorre almeno una delle seguenti condizioni:…* ***e)*** *il trattamento* ***è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento****…*".

Si rileva come alcune delle restanti condizioni previste dall'art. 6.1 del Regolamento UE 2016/679 (vedi lett. c): "*il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento"* e lett. b): "*il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*") debbano essere ricondotte – in relazione ai soggetti pubblici – all'esercizio delle funzioni istituzionali pubbliche che competono all'ente stesso.

Il successivo art. 6.3 stabilisce che: "***La base su cui si fonda il trattamento*** *dei dati di cui al paragrafo 1, lettere c) ed e),* ***deve essere stabilita****:*
a) dal diritto dell'Unione; o
b) ***dal diritto dello Stato membro cui è soggetto il titolare del trattamento****.*
La finalità del trattamento *è determinata in tale base giuridica o,* ***per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), 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****…*".
Infine, l'art. 2-*ter* del D. Lgs. n. 196/2003 puntualizza che: "***La base giuridica*** *prevista dall'art. 6, paragrafo 3, lett. b),* ***è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento***". Quindi, anche per il mero trattamento (ovvero, per compiere operazioni diverse dalla comunicazione o diffusione) di dati "comuni", il soggetto pubblico necessita di una norma di legge o di regolamento (nei termini sopra descritti).

Nel caso in cui il trattamento concerna particolari categorie di dati personali, nonché dati relativi a condanne penali e reati, occorrerà rispettare, altresì, i presupposti di cui agli artt. 9 e 10 del Regolamento UE 2016/679, nonché quelli stabili dagli artt. 2-*sexies*, 2-*septies* e 2-*octies*, del D. Lgs. n. 196/2003, illustrati nel prosieguo.

2.6 Consenso dell'interessato e trattamento di dati personali da parte della Pubblica Amministrazione

Il considerando n. 43 del Regolamento UE 2016/679 precisa che: "*Per assicurare la libertà di espressione del consenso, è opportuno che* ***il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali*** *in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento,* ***specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica****. Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione*".
Conseguentemente, quindi, i soggetti pubblici non dovrebbero avvalersi del presupposto di cui all'art. 6, paragrafo 1, lett. a) (consenso dell'interessato), salvo casi eccezionali da valutare attentamente (in tali casi, per quanto ovvio, dovranno applicarsi tutte le relative disposizioni normative).

2.7 Comunicazione e diffusione

La comunicazione è un'operazione del trattamento che consiste nel portare i dati personali a conoscenza di uno o più soggetti determinati (identificabili in modo univoco e determinato).

Non si considera comunicazione lo scambio di dati tra Strutture interne dell'Amministrazione, o tra queste ultime e soggetti esterni individuati come Responsabili o persone autorizzate al trattamento (nell'ambito di attività di *outsourcing*, o in base ad atto convenzionale). In tal caso anche i soggetti esterni che collaborano con la Provincia vengono considerati "articolazioni" della stessa.

La diffusione è un'operazione del trattamento che consiste nel portare i dati personali a conoscenza di soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione, o consultazione.

Tipiche forme di diffusione sono quelle che si realizzano, ad esempio, tramite registri o albi pubblici, con la pubblicazione delle deliberazioni della Giunta provinciale e delle determinazioni dei Dirigenti ai sensi dell'art. 31 della legge provinciale 1992, n. 23, nonché con le pubblicazioni ai sensi del D. Lgs. n. 33/2013 e s.m.i..

Sia la consultazione di dati personali contenuti in un sistema informativo (o nelle banche dati co-gestite da più Strutture), che la visualizzazione occasionale di dati non pertinenti o eccedenti rispetto ai propri compiti, non legittima forme di comunicazione e/o diffusione degli stessi che non siano strettamente necessarie ai fini istituzionali. Analogamente, il fatto che il dato personale (o il documento che lo contiene) sia qualificabile come "pubblico" non consente, di per sé, la diffusione dello stesso.

2.8 Ulteriori presupposti che legittimano la comunicazione e la diffusione dei dati personali da parte dei soggetti pubblici e il trattamento dei dati "particolari" e relativi a "condanne penali e reati"

Relativamente ai dati diversi da quelli "particolari" e relativi a "condanne penali e reati", l'art. 2-*ter*, comma 2, del D. Lgs. n. 196/2003 stabilisce che: "***La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nella particolari categorie*** *di cui all'articolo 9 del Regolamento* ***e di quelli relativi a condanne penali e reati*** *di cui all'articolo 10 del Regolamento,* ***per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento***. *In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati*" (resta fermo, peraltro, quanto ulteriormente previsto dal D. Lgs. n. 82/2005 in materia di scambio di dati tra Pubbliche Amministrazioni, anche in merito alle modalità di fruizione).

Per quanto riguarda tutte le categorie di dati e, quindi, anche quelle riguardanti i dati "particolari" e relativi a "condanne penali e reati", fermi restando i presupposti di liceità di cui agli artt. 9 e 10 del Regolamento UE 2016/679 e agli artt. 2-*sexies*, 2-*septies* e 2-*octies* del D. Lgs. n. 196/2003, l'art. 2-*ter*, comma 3, dello stesso decreto legislativo prevede che: "*La* ***diffusione e la comunicazione di dati personali*** *trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri* ***a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste da una norma di legge o, nei casi previsti dalla legge, di regolamento***".

In particolare, l'art. 9.2, lett. g), del Regolamento UE 2016/679 consente il trattamento dei dati "particolari" quando "***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***".

L'art. 2-*sexies* del D. Lgs n. 196/2003, di conseguenza, stabilisce che: "***I trattamenti delle categorie particolari di dati personali*** *di cui all'articolo 9, paragrafo 1, del Regolamento,*

necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g)*, del medesimo articolo,* ***sono ammessi qualora siano previsti*** *dal diritto dell'Unione europea ovvero, nell'ordinamento interno,* ***da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato***".

Fermo restando quanto previsto da ulteriori disposizioni legislative, si intendono finalità di rilevante interesse pubblico quelle previste dal comma 2 del predetto art. 2-*sexies*, di seguito elencate:

"*a) accesso a documenti amministrativi e accesso civico;*

b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;

c) tenuta di registri pubblici relativi a beni immobili o mobili;

d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;

e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;

f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;

g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;

i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;

l) attività di controllo e ispettive;

m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

n) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

o) rapporti tra i soggetti pubblici e gli enti del terzo settore;

p) obiezione di coscienza;

q) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

s) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;

u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva".

L'art. 10 del Regolamento UE 2016/679 dispone che: "*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"*.

Il comma 5, dell'art. 2-*octies*, del D. Lgs. n. 196/2003, estende le disposizioni dell'art. 2-*sexies* dello stesso decreto anche al trattamento dei dati relativi a "condanne penali e reati" quando avviene sotto il controllo dell'autorità pubblica.
Fermo restando come l'art. 4 del D. Lgs. n. 196/2003 sia stato abrogato, il predetto art. 4, comma 1, lett. e), individuava come "dati giudiziari" (oggi dati relativi a "condanne penali e reati") "*i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale*". Sarà necessario, dunque, effettuare una valutazione di compatibilità con quanto disposto dal Regolamento UE 2016/679.

Recependo la facoltà di cui all'art. 9.4 del Regolamento UE 2016/679, l'art. 2-*septies* del D. Lgs. n. 196/2003, relativamente ai dati sanitari, genetici e biometrici, stabilisce che:
"*In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento,* ***i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo****". "Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalità del trattamento e possono individuare, in conformità a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati è consentito. In particolare,* ***le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati***". "***Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del regolamento, o altre cautele specifiche***". "*Nel rispetto dei principi*

in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, è ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo". "***I dati personali* sanitari, biometrici e genetici *non possono essere diffusi***".

L'art. 22, comma 11, del D. Lgs. n. 101/2018, prevede che sino all'adozione delle corrispondenti misure di garanzia di cui al suddetto art. 2-*septies*, "*le disposizioni... di cui al decreto legislativo n. 196 del 2003, relative al trattamento di dati genetici, biometrici o relativi alla salute continuano a trovare applicazione, in quanto compatibili con il Regolamento (UE) 2016/679*".

Inoltre, l'art. 36.5 del Regolamento UE 2016/679 dispone che, nonostante quanto previsto al paragrafo 1, "*il diritto degli Stati membri può prescrivere che* ***i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico****, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica*".
In attuazione di tale disposizione (per quanto parzialmente modificativa, non trattandosi di autorizzazione preliminare, bensì di provvedimento di natura generale), l'art. 2-*quinquiesdecies* del D. Lgs. n. 196/2003 prevede che: "***con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati*** *ai sensi dell'articolo 35 del Regolamento,* ***il Garante può****, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio,* ***prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare***".
A tale riguardo, l'art. 22, comma 3, del D. Lgs. n. 101/2018 sancisce che *"sino all'adozione dei corrispondenti provvedimenti generali di cui all'articolo 2-quinquiesdecies... i trattamenti di cui al medesimo articolo, già in corso alla data di entrata in vigore del presente decreto, possono proseguire qualora avvengano in base a espresse disposizioni di legge o regolamento o atti amministrativi generali, ovvero nel caso in cui siano stati sottoposti a verifica preliminare o autorizzazione del Garante per la protezione dei dati personali, che abbiano individuato misure e accorgimenti adeguati a garanzia dell'interessato*".
In particolare, il successivo comma 4 prevede che "*a decorrere dal 25 maggio 2018, i provvedimenti del Garante... continuano ad applicarsi, in quanto compatibili con il suddetto regolamento*" UE 2016/679 e con le disposizioni del D. Lgs. n. 196/2003.

Infine, si evidenzia come, ai sensi dell'art. 2-*quater* del D. Lgs. n. 196/2003, **il Garante sia tenuto a promuovere "*l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al capo IX del Regolamento, ne verifica la conformità alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto*".**
Il rispetto delle disposizioni contenute nelle Regole deontologiche "*costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali*" (sul punto, vedasi anche l'art. 111 del D. Lgs. 196/2003 per i trattamenti in ambito lavorativo).
Merita, quindi, di essere precisato come i Codici deontologici allegati A.2, A.3 e A.4 al D. Lgs. n. 196/2003 saranno oggetto di revisione da parte del Garante, nonché rinominati, per l'appunto, "Regole deontologiche". Pertanto, il trattamento effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, dovrà rispettare le disposizioni previste dall'art. 97 all'art. 110-*bis* del D. Lgs. n. 196/2003 e relative Regole deontologiche. Con comunicato stampa del 24/12/2018 il Garante ha informato di aver aggiornato e corretto tali Codici deontologici.
L'art. 21, comma 4, del D. Lgs. n. 101/2018 (a cui si rinvia per ulteriori dettagli) stabilisce che "*sino all'adozione delle regole deontologiche e delle misure di garanzia di cui agli articoli 2-quater e 2-septies del Codice in materia di protezione dei dati personali... producono effetti, per la*

corrispondente categoria di dati e di trattamenti, le autorizzazioni generali di cui al comma 2 e le pertinenti prescrizioni individuate con il provvedimento di cui al comma 1". Con avviso pubblico di data 13/12/2018 il Garante ha comunicato di aver completato la revisione delle nove Autorizzazioni generali e che "*in base all'analisi effettuata, quattro autorizzazioni hanno cessato completamente i loro effetti, in particolare: Autorizzazione generale n. 2/2016…; n. 4/2016…; n. 5/2016…; n. 7/2016. Sono state invece individuate cinque autorizzazioni che contengono specifiche prescrizioni compatibili con il nuovo assetto normativo: Autorizzazione generale n. 1/2016 al trattamento dei dati sensibili nei rapporti di lavoro; ...n. 3/2016; ...n. 6/2016; Autorizzazione generale n. 8/2016 al trattamento dei dati genetici; Autorizzazione generale n. 9/2016 al trattamento dei dati personali effettuato per scopi di ricerca scientifica*" (v. *newsletter* n. 448/2018), avviando una consultazione pubblica prima della loro approvazione definitiva.

2.9 Interpretazione della normativa nazionale in tema di protezione dei dati personali

Il D. Lgs. n. 196/2003 e ogni disposizione dell'ordinamento nazionale devono essere interpretate e applicate in conformità alla disciplina dell'Unione europea in materia di protezione dei dati personali. Ciò comporta l'obbligo, in capo ad ogni Preposto del trattamento, di verificare, al momento della relativa applicazione, che la normativa nazionale in tema di protezione dei dati personali non sia in contrasto con il Regolamento UE 2016/679 e con i relativi pareri del Comitato europeo per la protezione dei dati personali.
Analogamente, anche la normativa provinciale dovrà risultare conforme alla disciplina in materia di protezione dei dati personali (v. anche Corte Cost., sent. n. 271/2005).

2.10 Modalità per interloquire con l'Autorità di controllo

Ove la normativa (o le istruzioni del Garante) non richiedano specifiche modalità, è sempre opportuno utilizzare strumenti in grado di fornire prova della data di trasmissione e della ricezione da parte dell'Autorità. In taluni casi, infatti, il decorso dei termini (di risposta) da parte dell'Autorità può ritenersi silenzio-assenso (v. art. 36.4 del Regolamento UE 2016/679 e art. 154, comma 5, del D. Lgs. 196/2003; v. art. 2-*ter*, comma 2, del D. Lgs. 196/2003), mentre in taluni altri casi le iniziative assunte dal Titolare (*post* decorso dei suddetti termini e in assenza di risposta dell'Autorità) sembrerebbero esenti da punibilità (v. art. 36.1/2/3 del Regolamento UE 2016/679).

3. MISURE DI SICUREZZA ORGANIZZATIVE

3.1 Considerazioni generali

Le misure di sicurezza sono costituite dal complesso delle misure tecniche ed organizzative volte a ridurre, al minimo, i rischi di:

- distruzione o perdita, anche accidentale, dei dati (che integra una violazione della disponibilità dei sistemi e dei dati);
- accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta, divulgazione non autorizzata (che integrano una violazione della riservatezza dei sistemi e dei dati);
- modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole (che integra una violazione della integrità dei sistemi e dei dati).

Ai sensi dell'art. 32 del Regolamento "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*
a) la ***pseudonimizzazione*** *e la* ***cifratura*** *dei dati personali;*
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".
Pertanto, rispetto al previgente Codice, che stabiliva altresì misure minime di sicurezza vincolanti e predeterminate (che, peraltro, potranno ancora essere adottate per prevenire specifici rischi), in coerenza con la logica di *accountability* (autoresponsabilizzazione) l'attuale normativa prevede che il Titolare debba adottare misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio connesso ai trattamenti.

In tale ottica, i Responsabili esterni (*in primis* Trentino Digitale S.p.a. e coloro che gestiscono, per conto della Provincia, il *Sistema informativo elettronico trentino - SINET*, di cui quello provinciale è parte, nonché le infrastrutture, i sistemi e gli applicativi utilizzati per i trattamenti dall'amministrazione provinciale) sono tenuti ad adottare tutte le misure idonee a garantire un livello di sicurezza adeguato ai rischi dei trattamenti.

La mancata adozione delle misure di sicurezza può dar luogo a responsabilità civile.
L'articolo 82 del Regolamento UE 2016/679 stabilisce, infatti, che "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".
Ai sensi dell'art. 83.4 del Regolamento UE 2016/679, alla mancata adozione adozione di tali misure può altresì conseguire una sanzione amministrativa sino a 10 mln di Euro.

Peraltro, deve evidenziarsi come l'art. 166, comma 2, del D. Lgs. n. 196/2003 operi un rinvio alle sanzioni più severe (sino a 20 mln di Euro) di cui all'art. 83.5 del Regolamento UE 2016/679, in caso di violazione delle misure di garanzia prescritte dal Garante ai sensi gli articoli 2-*quater* e 2-*septies* del D. Lgs. n. 196/2003. In tale ultimo caso, inoltre, è configurabile la responsabilità penale di cui all'art. 170 del D. Lgs. n. 196/2003.

Poiché il parametro previsto dalla normativa, per l'accertamento dell'eventuale responsabilità civile, è quello dell'adeguatezza delle misure di sicurezza, le stesse dovranno essere valutate da parte dei Dirigenti e, se del caso, specificamente implementate con ulteriori misure atte a garantire livelli di protezione maggiori e più conformi al contesto in cui si svolgono i trattamenti, tenendo costantemente conto dell'evoluzione tecnologica degli strumenti di protezione, dei nuovi rischi e dei più recenti provvedimenti in materia delle varie Autorità di settore (tra cui, il Garante, Agid ed Anac).

Le misure di sicurezza tecnico-informatiche sono descritte nella Sezione II; a tal proposito, si rammenta che Agid (Agenzia per l'Italia Digitale) ha prescritto, con circolare n. 2/2017 ("*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni*"), l'adozione di una serie di misure minime da adottare entro il 31 dicembre 2017. Inoltre, la stessa Autorità è intervenuta (con apposite Linee Guida, a cui si rinvia) anche sugli aspetti di sicurezza relativi ad ulteriori specifiche questioni. Nel presente Capitolo 3 invece, sono sintetizzati i principali e non esaustivi accorgimenti, nonché le misure organizzative da adottare nel trattamento dei dati personali.

3.2 Prescrizioni operative finalizzate alla riduzione dei rischi

Tutti i dipendenti sono tenuti, nell'ambito dei rispettivi compiti, a garantire la sicurezza delle informazioni trattate, attraverso la salvaguardia della loro (a) riservatezza, (b) integrità e (c) disponibilità, attenendosi anche alle "Istruzioni organizzative e comportamentali", specificate nei successivi Paragrafi 3.2.1 e 3.2.2.

I dipendenti, in particolare, devono:
a) assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati a trattarle;
b) salvaguardare l'esattezza, la completezza e l'aggiornamento delle informazioni.
I sistemi e le reti d'informazione sono sottoposti a rischi interni ed esterni; quindi, è necessario che i dipendenti siano consapevoli del fatto che, a causa dell'interdipendenza tra sistemi, falle in materia di sicurezza, che riguardano anche solo un componente del sistema, possano propagare i loro effetti fino ad incidere, gravemente, sull'integrità dei sistemi, delle reti, delle banche dati, degli archivi, nonché arrecare danni a terzi.
I comportamenti da adottare devono tener conto della natura dei dati, delle specifiche caratteristiche del trattamento, della probabilità e gravità del rischio per i diritti e le libertà delle persone fisiche, nonché delle conoscenze acquisite in base al progresso tecnico e dei relativi costi di attuazione.

3.2.1 Istruzioni organizzative e comportamentali relative a trattamenti effettuati con strumenti informatici

Oltre a quanto specificamente previsto nella Sezione II del presente documento, appositamente dedicata alla misure di sicurezza tecnico-informatiche, si raccomanda il rispetto dei seguenti comportamenti:

A. Conservare i supporti estraibili (cdrom, chiavi usb, ecc.) in un luogo sicuro

Per i supporti estraibili si applicano gli stessi criteri stabiliti per i documenti cartacei, dovendo, però, considerare l'ulteriore rischio che il loro smarrimento (eventualmente dovuto anche a un furto) possa passare più facilmente inosservato. A meno che non vi sia certezza che non contengano dati personali, quindi, tali supporti dovranno essere riposti sotto chiave non appena terminato l'utilizzo.

B. Utilizzare le password

Esistono molteplici categorie di *password*, ognuna delle quali è caratterizzata da una specifica funzione.

- La *password* di accesso al computer impedisce l'utilizzo, improprio, della postazione in caso di assenza dall'ufficio.
- La *password* di accesso alla "rete" impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'ufficio.
- La *password* di programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
- La *password* del salva-schermo (*screen saver*), infine, impedisce che, nel caso di momentanea assenza, una persona non autorizzata possa accedere alle risorse del computer.

C. Come deve essere scelta la password

La parola chiave, per l'accesso al sistema, deve essere composta da almeno otto caratteri di cui almeno un carattere maiuscolo e uno numerico; nel caso in cui tale regola non possa essere rispettata, si deve utilizzare una *password* sicura, ovvero una *password* che non possa essere scoperta da un programma o una persona in un breve lasso di tempo. La *password* deve essere modificata al primo utilizzo e, successivamente, ogni sei mesi; per il trattamento dei dati "particolari" e relativi a "condanne penali e reati" la *password* deve essere modificata ogni tre mesi. L'Amministrazione, ove possibile, adotterà meccanismi di cambio *password* di *default*, con le modalità e i vincoli ritenuti opportuni, o richiesti da provvedimenti specifici.

D. Non permettere a terzi di conoscere le password

Anche se molti programmi non ripetono in chiaro la *password* sullo schermo, nel momento in cui la stessa viene digitata potrebbe essere letta osservando la battitura dei tasti. Porre attenzione che nessuno possa apprendere la propria *password*.

E. Come custodire le password in un luogo sicuro

Non lasciare traccia scritta della *password*, tanto più vicino alla relativa postazione di lavoro.

F. Come evitare l'identificazione della password

I. Non comunicare, a nessuno, la *password*. Lo scopo principale per cui si adotta una *password* consiste nell'assicurare che nessun altro possa utilizzare le risorse informatiche, o possa farlo a nome dell'utente a cui la *password* è associata.
II. Non scegliere *password* che si possano trovare nei dizionari delle lingue più diffuse (ad esempio inglese o spagnolo) oltre a quello italiano. Su alcuni sistemi è possibile testare le *password* per verificare quella più adeguata.
III. Non usare il nome utente come *password*, né alcun riferimento legato alla propria sfera personale.
IV. Una frode molto diffusa, che si avvale della posta elettronica, è il *phishing*. Si tratta di una metodologia di attacco informatico che si può riassumere nelle seguenti fasi:

- il *phisher* spedisce, all'utente, una *e-mail* che simula, nella grafica e nel contenuto, un'istituzione nota al destinatario (per esempio la sua banca, il suo *provider web*, un sito di aste *online* a cui è iscritto);
- la *mail* contiene, quasi sempre, avvisi concernenti particolari situazioni o problemi verificatisi con il proprio conto corrente/*account* (ad esempio un addebito abnorme, la scadenza dell'*account*, ecc.), oppure un'offerta di denaro;
- la *mail* invita il destinatario ad accedere ad un *link*, indicato nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente, o con la società dei quali il messaggio simula la grafica e l'impostazione del sito;

- il *link* fornito, tuttavia, non consente l'accesso ad alcun sito *web* ufficiale, bensì ad una copia fittizia, apparentemente simile al sito ufficiale, situata in un *server* controllato dal *phisher*, allo scopo di richiedere e ottenere, dal destinatario, i suoi dati personali, solitamente con la motivazione di una conferma, o della necessità di effettuare un'autenticazione al sistema; queste informazioni vengono memorizzate, dal *server* gestito dal *phisher* e, quindi, finiscono nella disponibilità del malintenzionato;
- il *phisher* utilizza questi dati per acquistare beni, trasferire somme di denaro, o anche solo come "ponte" per ulteriori attacchi.

Si consiglia, quindi, di prestare molta attenzione all'autenticità di *e-mail* che rinviano a siti che richiedano l'introduzione di dati personali, in modo tale da utilizzare in sicurezza le apparecchiature informatiche messe a disposizione dal datore di lavoro. In caso di dubbio, contattare l'indirizzo di posta dedicato alle problematiche di sicurezza (sicurezza@infotn.it).

G. Prestare attenzione alle stampe di documenti riservati

Non consentire l'accesso alle fotocopie da parte di soggetti non autorizzati; se la stampante non si trovasse nel proprio ufficio, è necessario recarsi immediatamente a ritirare i documenti stampati. Distruggere, personalmente, i documenti quando non sono più necessari. Qualora una stampante si bloccasse, è necessario assicurarsi (eventualmente, coinvolgendo il referente informatico) che non restino dati personali nella memoria della stampante, i quali potrebbero essere nuovamente inviati in stampa, una volta che le funzionalità della stampante fossero state ripristinate.

H. Non lasciare traccia dei dati riservati

Quando si cancella un *file*, i dati non vengono effettivamente rimossi, ma soltanto marcati come non utilizzati e, pertanto, risultano facilmente recuperabili. La formattazione, o la sovrascrittura, rendono più complesso il recupero dei dati. Solo l'utilizzo di un apposito programma garantisce che, sul supporto estraibile, non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un nuovo supporto estraibile.

I. Prestare attenzione all'utilizzo dei dispositivi mobili (notebook, tablet, smartphone, ecc.)

I *pc* portatili sono un facile bersaglio, per i ladri, anche al di fuori dell'ufficio. Qualora vi fosse la necessità di gestire dati personali attraverso un portatile, è opportuno valutare, in relazione alla natura dei dati e alle modalità del trattamento, se installare un programma di cifratura e pseudonimizzazione, utilizzando in ogni caso una procedura di *backup* periodico.

J. Non consentire l'utilizzo del computer a personale esterno, laddove non si abbia certezza della relativa identità

Personale esterno potrebbe avere la necessità di installare un nuovo *software/hardware* nel computer. E', quindi, necessario assicurarsi dell'identità della persona, nonché delle relative autorizzazioni ad operare sul *pc*.

K. Non usare apparecchiature non autorizzate

L'utilizzo di connessioni alternative non approvate e sconosciute (esempio reti *wifi* libere) su postazioni di lavoro collegate in rete, offre una porta d'accesso, dall'esterno, non solo al singolo *computer*, ma a tutta la rete; di conseguenza, tale comportamento è vietato. Per l'utilizzo di altre apparecchiature, è necessario consultare il Preposto al trattamento del relativo ufficio ed il referente informatico.

L. Non installare programmi non autorizzati

Solo i programmi istituzionali, o acquistati dall'Amministrazione con regolare licenza, sono autorizzati. Qualora l'attività lavorativa richiedesse l'utilizzo di programmi ulteriori rispetto a quelli già autorizzati, è necessario consultare il Preposto al trattamento del relativo ufficio ed il referente informatico.

M. Effettuare backup periodici

E' necessario memorizzare i dati di interesse lavorativo sui dischi U e Y, ove disponibili; in caso contrario, effettuare il *backup* periodico per i trattamenti non gestiti da Trentino Digitale S.p.a.

N. Regole volte a prevenire infezioni di virus

Prevenire un *virus* comporta un impiego di tempo di gran lunga inferiore rispetto alle attività di rimozione degli effetti prodotti; la mancata prevenzione, tra l'altro, potrebbe determinare la perdita irreversibile dei dati.

Cos'è un virus:
un *virus* è un programma in grado di propagarsi autonomamente e che può causare effetti dannosi. Alcuni *virus* si limitano a riprodursi, senza ulteriori effetti, mentre altri si limitano alla semplice visualizzazione di messaggi sul video; i più dannosi arrivano a rendere illeggibile parte o tutto il contenuto dei dischi di rete e locali.
Una tipologia particolare di *virus*, ad esempio, è il *ransomware*. Trattasi di un *malware* che, cifrando i *file* memorizzati sui dischi locali o di rete, ne impedisce la visualizzazione ed il conseguente utilizzo.

Come si trasmette un virus:

1. attraverso programmi;
2. attraverso le *macro* dei programmi di automazione d'ufficio;
3. attraverso supporti esterni (ad esempio chiavi *usb*), contenenti *file* non controllati da *antivirus*.

Azioni che possono generare un alto rischio di infezione da virus:

1. apertura di messaggi di posta elettronica provenienti da mittenti sconosciuti e contenenti allegati o collegamenti a siti *internet;*
2. copia di dati da supporti di memorizzazione;
3. *download* di dati, o di programmi, da *internet.*

Alcuni effetti provocati da virus:

1. effetti sonori e messaggi sconosciuti che appaiono sul video;
2. visualizzazione di nuove funzionalità sino a quel momento non disponibili;
3. riduzione inspiegabile dello spazio disco residuo;
4. rallentamenti inspiegabili del *pc*;
5. diffusione del *virus* su altre stazioni collegate al *network* aziendale;
6. impossibilità di accedere ai *file*, documenti, o al servizio (*denial of service*)
7. indecifrabilità del *file*, o documento.

Come prevenire i virus:

1. Usare soltanto programmi provenienti da fonti sicure
Copie sospette di programmi possono contenere *virus* o altro *software* dannoso. Ogni programma deve essere sottoposto a specifica scansione, prima di essere installato; non avvalersi di programmi non autorizzati, spesso utilizzati per trasmettere *virus*.
2. Non avviare il computer da supporto estraibile
Se il supporto estraibile fosse infettato, il *virus* si trasferirebbe nella memoria *RAM* e potrebbe espandersi ad altri *file*.
3. Verificare che il software antivirus sia aggiornato
La tempestività dell'azione di bonifica è essenziale per limitare i danni che un *virus* può causare; è fondamentale, quindi, che il programma *antivirus* sia aggiornato e, di conseguenza, in grado di

individuare le versioni più recenti dei *virus* in circolazione. Attualmente, per le macchine collegate in rete, tutti i sistemi *antivirus* della Provincia vengono gestiti da Trentino Digitale S.p.a., tramite un sistema di controllo che provvede a segnalare, al presidio di assistenza delle postazioni di lavoro, le macchine che non sono aggiornate; per le macchine non collegate in rete l'aggiornamento è affidato al *software antivirus* che si aggiorna appena le stesse si collegano ad *internet.*

Come evitare la diffusione dei virus:

1. Non diffondere messaggi di provenienza dubbia
Qualora si ricevessero messaggi di avviso di un nuovo *virus*, non prestare attenzione a tali comunicazioni: le *e-mail* di questo tipo sono qualificate, con terminologia anglosassone, *hoax* (termine spesso tradotto in italiano con "bufala"). Tale qualificazione non muta anche nel caso in cui il messaggio provenisse da tecnici informatici, nonché laddove si faccia riferimento a notizie provenienti da *software house*.
2. Non partecipare a "catene di S. Antonio" e operazioni similari
Analogamente, tutti i messaggi che invitano a "diffondere la notizia quanto più possibile", sono *hoax*.

L'uso della posta elettronica e di *internet* deve essere conforme a quanto previsto nell'apposito disciplinare, adottato dalla Giunta provinciale con deliberazione n. 1037/2010, sulla base del provvedimento del Garante dd. 1/03/2007. A tale proposito, si rinvia a quanto previsto nella Sezione II.

3.2.2 Istruzioni organizzative e comportamentali relative a trattamenti effettuati con strumenti cartacei

Il primo livello di protezione di qualunque sistema è quello fisico; sebbene un armadio chiuso a chiave possa, in molti casi, non costituire una protezione sufficiente, è anche vero che, se non altro, può costituire un primo ostacolo richiedendo, comunque, uno sforzo volontario, non banale, per aprirlo. Quando ci si allontana dall'ufficio, pertanto, è necessario chiudere i documenti a chiave nei cassetti e/o negli armadi; nel momento in cui documenti fossero conservati in armadi a vetri, è sempre meglio oscurarli (ad esempio, apponendo alle ante fogli di carta montati all'interno).

Le misure da adottare sono finalizzate a ridurre al minimo i rischi di:
- accesso fisico non autorizzato / illecita divulgazione dei dati;
- furto / alterazione dei dati da parte di malintenzionati;
- distruzione / perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

Preso atto di quanto previsto dall'art. 32 del Regolamento UE 2016/679 e della contestuale abrogazione degli articoli da 33 a 36 (ed allegato B) del previgente D. Lgs. n. 196/2003 (misure di sicurezza minime), le misure di seguito descritte hanno natura meramente indicativa e dovranno essere adeguate ed implementate, da parte del Preposto al trattamento, a seconda della natura dei dati trattati e dei potenziali rischi (ad esempio, dovrà essere valutata l'adozione di: serrature blindate, inferriate, sistemi di allarme, o di videosorveglianza).

La Struttura che effettua trattamenti di dati personali su supporto cartaceo, deve dotarsi di arredi (cassettiere, armadi, ecc.), muniti di meccanismi di serratura adatti a garantire la sicurezza, da destinare ad archivio dei documenti contenenti dati personali.
Pertanto, l'accesso agli archivi è consentito ai soli Preposti e ai relativi Addetti al trattamento.
I documenti possono essere estratti dall'archivio, e affidati alla custodia dell'Addetto, per il tempo strettamente necessario all'esecuzione del trattamento. L'Addetto garantisce la riservatezza e provvede al deposito in archivio, al termine delle operazioni.

Con riferimento alle particolari categorie di dati e ai dati riguardanti "condanne penali e reati", inoltre, l'accesso ai relativi archivi deve essere controllato, dovendosi altresì adottare le seguenti misure:
- la chiave deve essere custodita da personale a ciò specificamente incaricato dal Dirigente della Struttura;
- il personale incaricato della custodia delle chiavi è tenuto a riporle in un luogo non agevolmente accessibile da altri;
- l'archivio viene aperto e chiuso dal personale custode delle chiavi;
- i soggetti che possono accedere all'archivio, dopo l'orario di servizio, devono essere identificati e registrati.

In particolare, i dati genetici, biometrici e quelli idonei a rivelare stato di salute, vita sessuale, ovvero orientamento sessuale, devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Un archivio è soggetto al rischio di molteplici eventi pregiudizievoli, che possono provocare la distruzione, o il danneggiamento dei documenti. Al fine di ridurre al minimo tali rischi, le principali misure da adottare sono le seguenti:
- in sede di progettazione e di realizzazione di nuove strutture adibite a sede di uffici provinciali, ovvero in sede di ristrutturazione degli edifici esistenti, occorre considerare la necessità di collocare i locali adibiti ad archivio in luoghi sicuri, evitando ad esempio scantinati e piani seminterrati a rischio di allagamenti;
- nei locali adibiti ad archivio devono essere installati idonei dispositivi antincendio.

Con riferimento ai sistemi di videosorveglianza anzi citati, si rammenta che l'adozione e gestione di tali strumenti dev'essere conforme a quanto previsto nell'apposito disciplinare adottato dalla Giunta provinciale con deliberazione n. 2643/2008, nonché a quanto previsto nel provvedimento del Garante dell'8/04/2010, documenti ai quali si rinvia; a titolo di mero coordinamento e per favorire una migliore gestione delle procedure di sicurezza delle informazioni, si riportano alcuni precetti del citato provvedimento.

Nelle Strutture dove sono attivati sistemi di videosorveglianza, finalizzati alla protezione dei dipendenti, dei visitatori e del patrimonio, deve essere affissa apposita informativa che informi il pubblico della presenza degli impianti e delle finalità perseguite attraverso la videosorveglianza. I pannelli devono essere affissi in prossimità degli ingressi (prima del campo di azione della telecamera) ed essere visibili a chi vi accede (anche in orario notturno).
Nella gestione dei sistemi di videosorveglianza, inoltre, è necessario rispettare i seguenti principi:
a) limitazione delle modalità di ripresa delle immagini (memorizzazione, angolo visuale delle telecamere e limitazione della possibilità di ingrandimento dell'immagine), avendo attenzione alla individuazione del livello di dettaglio della ripresa dei tratti somatici delle persone, in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;
b) limitazione dei tempi di conservazione delle immagini (la conservazione dei dati personali dev'essere limitata alle ventiquattrore successive alla rilevazione, fatte salve alcune specifiche ipotesi (festività o chiusura uffici; richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria). In ogni caso, la conservazione dei dati non potrà superare la settimana, salvo specifica autorizzazione del Garante;
c) individuazione dei soggetti legittimati ad accedere alle registrazioni;
d) indicazione del soggetto e della Struttura a cui l'interessato può rivolgersi e dei diritti che può esercitare.

4. REGOLE GENERALI PER TUTTI I TIPI DI TRATTAMENTO

4.1 Principi fondamentali per il trattamento dei dati personali

Ogni trattamento di dati personali deve svolgersi nel rispetto delle seguenti indicazioni:
- va privilegiato, ove possibile, il trattamento di dati anonimi;
- se non è possibile perseguire le finalità del trattamento mediante dati anonimi, deve comunque essere garantita l'osservanza del principio di minimizzazione, come di seguito meglio specificato. Tale principio dev'essere garantito sin dall'origine del trattamento (*privacy by design*), anche mediante impostazione predefinita (*privacy by default*), ai sensi dell'art. 25 del Regolamento UE 2016/679.

Ai sensi degli articoli 5 e 29 del Regolamento UE 2016/679, i dati personali, inoltre, devono essere:
- trattati in modo lecito, corretto e trasparente ("liceità, correttezza e trasparenza");
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità ("limitazione della finalità");
- esatti e, se necessario, aggiornati ("esattezza");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione");
- conservati in una forma che permetta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione mediante misure tecniche e organizzative adeguate ("integrità e riservatezza")
- trattati da personale appositamente autorizzato ed istruito.

Per garantire la sicurezza dei dati personali:
- le riproduzioni di documenti equivalgono ai documenti stessi e, pertanto, sono gestite con le medesime cautele;
- qualunque prodotto dell'elaborazione di dati personali, ancorché non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, elaborazioni temporanee, ecc.), deve essere trattato con le stesse cautele che sarebbero riservate alla versione definitiva.

Le misure individuate nel presente documento si applicano anche ai collaboratori esterni della Provincia i quali, nell'ambito dei compiti loro affidati, procedono al trattamento di dati personali dell'Ente.

4.2 Principali obblighi derivanti dal Regolamento UE 2016/679

4.2.1 Informativa

Nel rispetto di quanto previsto dall'art. 12 del Regolamento UE 2016/679, l'informativa dev'essere concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre, quindi, utilizzare un linguaggio chiaro e semplice, specialmente se si tratta di minori. L'informativa è fornita, in linea di principio, per iscritto e con ogni mezzo appropriato, anche con mezzi elettronici.

L'informativa deve essere consegnata, all'interessato, secondo le modalità indicate negli articoli 13 e 14 del Regolamento UE 2016/679 e, se i dati sono raccolti presso l'interessato stesso, deve essere fornita prima dell'inizio del trattamento.

In particolare, in caso di raccolta presso l'interessato (art. 13 Regolamento UE 2016/679), il Titolare fornisce, allo stesso, almeno le seguenti informazioni: a) l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del Responsabile della protezione dei dati; c) le finalità del trattamento, nonché la base giuridica del trattamento stesso (qualora il Titolare intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui sono stati raccolti, fornisce tutte le informazioni anche in merito a tale ulteriore finalità); d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; e) ove applicabile, l'intenzione del Titolare del trattamento di trasferire dati personali a un Paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nei casi di cui agli articoli 46, 47 e 49, paragrafo 1, secondo comma, del Regolamento UE 2016/679, il riferimento alle garanzie appropriate od opportune ed i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Con riferimento alla precedente lettera c) e, in particolare, al trattamento per ulteriori finalità, (qualora (A.) l'ulteriore trattamento non avvenga a fini di archiviazione nell'interesse pubblico, a fini di ricerca scientifica o storica o a fini statistici o (B.) la base legittima per l'ulteriore trattamento non sia rappresentata da una previsione normativa) dovranno essere altresì forniti gli elementi per consentire all'interessato di valutare la "compatibilità" dell'ulteriore trattamento. Ogni successiva modifica del trattamento, inoltre, richiederà la consegna di una nuova informativa entro un tempo ragionevole dall'inizio del trattamento, per consentire all'interessato di esercitare i propri diritti (ad es., di opposizione).

Con riferimento alla precedente lettera d), considerato come nella categoria "destinatari" siano altresì ricompresi i Responsabili del trattamento, si è ritenuto di assicurare l'effettiva conoscibilità di tali soggetti mediante (nell'informativa) l'individuazione per macro-categorie di riferimento e il rinvio all'elenco dei Responsabili del trattamento, nonché la successiva affissione dello stesso elenco nella bacheca di ciascuna Struttura (ovvero, la pubblicazione nello specifico sito *internet*).

Per garantire un trattamento corretto e trasparente, nell'informativa devono essere riportate anche le seguenti ulteriori indicazioni: 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 dei dati personali che lo riguardano, o di opporsi al loro trattamento; c) qualora il provvedimento di cui all'art. 2-*septies* del D. Lgs. n. 196/2003 preveda, come ulteriore misura di garanzia per il trattamento dei dati genetici, il consenso dell'interessato (o, nei casi eccezionali in cui il consenso sia individuato come base legittima del trattamento), il diritto di revocarlo in qualsiasi momento; d) il diritto di proporre reclamo all'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, e, almeno in tali casi, le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze per l'interessato.

Le informazioni sopra riportate devono essere indicate anche in termini negativi (ad esempio, non sussiste comunicazione a terzi; non viene effettuata profilazione; i dati non sono trasferiti al di fuori della UE; ecc.). A tal fine, si ricorda che lasciare vuote le caselle dell'informativa (cioè, senza *flag*) è scorretto, in quanto non consente all'interessato di conoscere quali voci siano applicabili (tale ragionamento, infatti, non va confuso con i casi di consenso dell'interessato per determinati trattamenti, in cui preselezionare "di *default*" le caselle è illegittimo, impedendo la manifestazione del consenso stesso).

L'informativa non deve essere fornita se, e nella misura in cui, l'interessato dispone già delle informazioni.

Nel caso in cui i dati non siano raccolti presso l'interessato (art. 14 del Regolamento UE 2016/679) l'informativa deve contenere, in aggiunta a quelle specificate nell'articolo 13, le seguenti informazioni: le categorie di dati personali trattati; la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

Se i dati personali non sono raccolti presso l'interessato, l'informativa è fornita, al medesimo, entro un termine ragionevole dall'ottenimento dei dati, ovvero in occasione della prima comunicazione all'interessato stesso o non oltre la prima comunicazione ad altri destinatari e, comunque, non oltre un mese.

Ai sensi dell'art. 48 del D.P.R. 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), è obbligatorio inserire l'informativa nella modulistica per la presentazione delle dichiarazioni sostitutive di certificazione e di atto notorio. Fermi restando gli obblighi di consegna dell'informativa, in via generale, nella modulistica relativa alle istanze da presentare all'Amministrazione provinciale sarebbe preferibile inserire il testo dell'informativa stessa.

Il paragrafo 5, dell'articolo 14, del Regolamento UE 2016/679, stabilisce i casi in cui il medesimo articolo non si applica e, in particolare, quando:
"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,* ***o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento****. In tali casi, il titolare del trattamento 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 membro cui è soggetto il titolare del trattamento e* ***che 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 degli Stati membri, compreso un obbligo di segretezza previsto per legge".*

Eccetto il caso *sub* a), le rimanenti fattispecie sono applicabili esclusivamente nell'ipotesi di raccolta dei dati presso terzi (ovvero ottenuti da fonti pubbliche, o comunicati da terzi).

Per elevare il livello di trasparenza (*ex* art. 12 del Regolamento UE 2016/679) e relativa *accountability*, anche prendendo spunto dal provvedimento del Garante dd. 19/06/2008 (doc. *web* 1526724), nonché dalle Linee Guida del Comitato europeo per la protezione dati sulla trasparenza, la Provincia ha ritenuto opportuna – da parte di ogni singola Struttura – la predisposizione e pubblicazione, sul proprio sito istituzionale, di un'informativa generale, in modo tale da fornire, ai cittadini e ai fornitori/collaboratori/consulenti, un'immediata e complessiva rappresentazione delle possibili attività di trattamento.
Pertanto, tenendo presente le attività di propria competenza, la Struttura deve riassumere, in modo chiaro ed in forma adeguatamente concisa, i possibili trattamenti, in modo che l'interessato possa comprendere, nel momento in cui entrasse in rapporto con la Struttura stessa, quali dati potrebbe dover fornire (o quali dati la Struttura potrebbe ricevere da fonti pubbliche o da terzi), le finalità e le basi giuridiche per cui gli stessi sarebbero trattati, se potrebbero o meno essere comunicati o diffusi, ecc.

Nell'informativa generale, pertanto, non è necessario distinguere trattamento per trattamento, ovvero specificare, volta per volta, quali dati siano trattati per determinate finalità e quali per altre, oppure quali siano comunicati e quali no. E' sufficiente una rappresentazione complessiva, sia pur effettiva e veritiera, dei potenziali trattamenti.
La predisposizione e pubblicazione dell'informativa generale, ovviamente, non esime in alcun modo dalla corretta, puntale e precisa, predisposizione e successiva consegna dell'informativa, *ex* artt. 13/14 del Regolamento.

Infine, come di seguito meglio precisato, una particolare forma di informativa è prevista dall'art. 26 del Regolamento UE 2016/679, ovvero in caso di co-titolarità, nonché dall'art. 11.2 dello stesso Regolamento.

4.2.2 Progettazione e impostazione predefinita della protezione dei dati

L'articolo 25, paragrafo 1, del Regolamento UE 2016/679 specifica che il Titolare, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi connessi al medesimo, "***sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso****… mette in atto misure tecniche ed organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione...*".

Il paragrafo 2, sempre nella medesima ottica, prescrive misure tecniche ed organizzative adeguate "*...per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento… In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*".

La normativa europea prevede, dunque, sin dall'origine del trattamento, oltre che nel corso del medesimo, misure volte a utilizzare solo i dati necessari alle finalità dello stesso, nonché a limitare la conoscibilità dei dati anche nell'ambito della stessa organizzazione del Titolare e a definirne il periodo di conservazione.

Le principali misure strumentali, a tale scopo, sono la piena applicazione del principio di minimizzazione dei dati rispetto alla finalità prefissata e la pseudonimizzazione, ovvero l'impossibilità (ottenuta, ad esempio, generando un codice che ricostruisce il dato, ed il suo collegamento all'interessato, soltanto se necessario) di conoscere i dati identificativi del soggetto interessato senza l'utilizzo di ulteriori informazioni aggiuntive, tenute separate dai primi. L'"anonimizzazione" (processo che impedisce in via irreversibile di riferire le informazioni all'interessato), invece, costituisce l'ambito entro il quale non si applica il Regolamento UE 2016/679.

I responsabili delle Strutture provinciali, pertanto, dovranno garantire che vengano trattati solo i dati effettivamente necessari all'esercizio delle finalità istituzionali e siano adottate, quando ritenute necessarie/opportune, idonee soluzioni che consentano di separare i dati identificativi degli interessati da altre informazioni aggiuntive che li riguardano.

4.2.3 Formazione

L'articolo 29 del Regolamento UE 2016/679 recita: *"Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali* ***non può trattare tali dati se non è istruito in tal senso*** *dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

L'articolo 32 del Regolamento (intitolato "Sicurezza del trattamento"), a propria volta, stabilisce, al paragrafo 4, che "*Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque*

agisca sotto la loro autorità e abbia accesso a dati personali ***non tratti tali dati se non è istruito in tal senso*** *dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

Appare chiaro come il legislatore dell'Unione europea abbia introdotto, a carico dei Titolari e Responsabili del trattamento, un propedeutico e condizionante obbligo di formazione che, stante le espressioni utilizzate, riguarda tutto il personale della Provincia. Tale obbligo di formazione, come facilmente desumibile dal già citato articolo 32 – che non a caso è intitolato "Sicurezza del trattamento" – è palesemente annoverabile tra le misure di sicurezza che Titolare e Responsabile del trattamento sono tenuti ad attuare.

I responsabili delle Strutture provinciali devono partecipare alle iniziative che verranno organizzate per assolvere, nei loro riguardi, l'obbligo di formazione in tema di protezione dei dati personali che, per propria natura, deve essere inteso come "continuo", nonché garantire che venga adeguatamente preparato tutto il personale delle Strutture di appartenenza mediante corsi, appositamente organizzati, che tengano conto dei rispettivi ruoli e livelli di competenza.

4.2.4 Notifica delle violazioni dei dati personali (*data breach*)

L'articolo 4, n. 12, del Regolamento UE 2016/679 definisce 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*".

L'articolo 33 del Regolamento UE 2016/679 prevede che il Titolare debba notificare, all'Autorità di controllo, le violazioni di dati personali di cui venga a conoscenza, "senza ingiustificato ritardo" e, ove possibile, entro 72 ore dalla scoperta della violazione, ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati (che spetta al Titolare; sul punto, vedasi anche le indicazioni fornite dal Comitato europeo per la protezione dei dati, nel WP 250).

Il predetto "considerando 85" del Regolamento UE 2016/679 detta alcuni esempi di cosa debba intendersi per rischio per i diritti e le libertà degli interessati ("*perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*").

Ai sensi dell'art. 34 del Regolamento UE 2016/679, se la probabilità di tale rischio è elevata, si dovranno informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo"; i contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esaustiva, dagli artt. 33 e 34 del Regolamento UE 2016/679. In particolare, la notifica deve contenere almeno: 1) la descrizione della natura della violazione (inclusi, se possibile, categorie e numero approssimativo di interessati, nonché categorie e numero approssimativo di registrazioni di dati); 2) nome e dati di contatto del responsabile della Struttura, o del Responsabile della protezione dei dati o di chi possa fornire informazioni più complete o dettagliate; 3) le probabili conseguenze della violazione dei dati personali; 4) le misure adottate, o di cui si propone l'adozione, per contrastare la violazione e ridurne i possibili effetti negativi.

I Dirigenti delle Strutture provinciali, nell'adempimento dell'obbligo richiamato, potranno farsi assistere, come previsto dall'articolo 28, paragrafo 3, lettera f), del Regolamento UE 2016/679, dal Responsabile del trattamento (Trentino Digitale S.p.a. o, eventualmente, altro Responsabile esterno).

Nell'ipotesi in cui il responsabile della Struttura provinciale accertasse una violazione di dati personali, è tenuto a comunicare l'evento al Responsabile esterno del trattamento (Trentino Digitale S.p.a. o altro Responsabile esterno), immediatamente e comunque non oltre entro 24 ore dalla conoscenza, qualora i sistemi informativi e/o gli applicativi utilizzati siano gestiti e messi a disposizione della Provincia, dalla Società di sistema o da diverso Responsabile esterno, in modo che quest'ultimo, entro le successive 48 ore, (a) possa effettuare, congiuntamente alla Struttura provinciale, un'adeguata istruttoria, (b) possa verificare se la violazione debba essere, o meno, notificata e (c) possa inviare l'eventuale notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati (tramite il modello predisposto dalla Struttura competente in tema di protezione dei dati). Il Responsabile esterno deve trasmettere tutte le violazioni (sia quelle notificate, che quelle non notificate) alla Struttura provinciale competente in materia di protezione dei dati personali.
Nel caso di cui sopra, qualora la violazione fosse accertata dal Responsabile esterno, quest'ultimo dovrà immediatamente riferire l'evento, alla Struttura provinciale coinvolta, attivando il processo sopra descritto.

Qualora, invece, la violazione di dati personali riguardasse sistemi informativi e/o applicativi "interni" (gestiti, cioè, in autonomia dalla singola Struttura provinciale), o fosse connessa all'organizzazione della medesima Struttura (ad es. accesso abusivo agli uffici o agli archivi cartacei, allagamenti, incendi, violazioni di dati causati dal comportamento del personale, ecc.), a integrazione di quanto già precisato nella circolare prot. n. 205959 del 9/04/2018, spetterà al Dirigente della Struttura provinciale (ferma restando l'assistenza del Responsabile del trattamento), entro 48 ore dalla scoperta della violazione, (a) compiere un'adeguata istruttoria e verificare se la violazione debba o meno essere notificata e (b) (se del caso) compilare il modello di notifica della violazione ed inoltrarlo alla Struttura provinciale competente in materia di protezione dei dati personali, la quale provvederà a trasmetterlo all'Autorità di controllo entro le ulteriori successive 24 ore.
I responsabili delle Strutture provinciali devono provvedere, se del caso, alla comunicazione della violazione agli interessati, *ex* art. 34 del Regolamento UE 2016/679, secondo i contenuti previsti dallo stesso articolo.

In ogni caso, il Titolare è tenuto a documentare tutte le violazioni di dati personali subite, anche se non notificate all'Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze, le conseguenze e i provvedimenti adottati. Per tali ragioni, presso l'Ufficio Organizzazione e gestione della privacy è conservato un fascicolo che raccoglie tutte le violazioni documentate dalle Strutture e dai Responsabili esterni.

I modelli di notifica e di comunicazione sono stati predisposti dall'Ufficio Organizzazione e gestione della privacy ed allegati alla presente deliberazione.

4.2.5 Valutazione d'impatto sulla protezione dei dati

La valutazione d'impatto sulla protezione dei dati è un processo finalizzato a descrivere il trattamento, valutarne la necessità e proporzionalità, nonché a individuare e gestire i rischi per i diritti e le libertà delle persone, derivanti dal trattamento stesso, individuando le misure necessarie per affrontarli. Tale valutazione, quindi, è anche un processo volto a garantire e dimostrare la conformità al Regolamento UE 2016/679 (principio di *accountability*).

L'articolo 35 del Regolamento UE 2016/679 prevede che il Titolare, "*quando un tipo di trattamento, **allorché prevede in particolare l'uso di nuove tecnologie**,…può presentare un rischio elevato per i diritti e le libertà delle persone fisiche,… effettua*, ***prima di procedere al trattamento**, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*". La valutazione d'impatto, dunque, si colloca, cronologicamente, all'inizio del trattamento, ponendosi,

in tal modo, quale misura di attuazione della cd. *privacy by design* (articolo 25 del Regolamento UE 2016/679).

Il processo di valutazione d'impatto è obbligatoriamente richiesto (articolo 35, paragrafo 2, del Regolamento UE 2016/679) nel caso di: "*a)…valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b)…trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c)…sorveglianza sistematica su larga scala di una zona accessibile al pubblico*".

Ai sensi della normativa europea, quindi, ogni Titolare deve individuare (in aggiunta a quelli qualificati tali dal legislatore europeo), attraverso l'analisi dei trattamenti, quelli c.d. a "rischio elevato" e, in un secondo momento, effettuare la valutazione d'impatto di questi ultimi sulla protezione dei dati personali. Il contenuto inderogabile della valutazione d'impatto è precisato (descrizione sistematica dei trattamenti e relative finalità; necessità e proporzionalità dei trattamenti; valutazione dei rischi per i diritti e le libertà degli interessati; misure previste per affrontare i rischi) dall'articolo 35, paragrafo 7, del Regolamento UE 2016/679. Qualora dalla valutazione d'impatto emerga che il trattamento, in assenza di misure di sicurezza adottate per attenuare il rischio, continui a presentare un rischio elevato, il Titolare, prima di effettuare (o proseguire) il trattamento, deve consultare l'Autorità di controllo (vedi art. 36, paragrafi 1, 2 e 3, del Regolamento UE 2016/679).

Alla luce delle complesse indicazioni del Comitato europeo per la protezione dei dati personali, del provvedimento del Garante n. 467/2018 All. 1, dell'ampiezza ed eterogeneità delle funzioni provinciali, la Provincia ha prudenzialmente ritenuto, come espressamente suggerito dal Comitato sopracitato, di applicare la valutazione d'impatto a tutti i trattamenti.

Sulla base di quanto in precedenza specificato ed allo scopo di favorire la corretta esecuzione della valutazione d'impatto, si precisa che la medesima dovrà, in particolare, essere effettuata, oltre che nei confronti di tutti i trattamenti in corso e di quelli nuovi, anche nelle seguenti ipotesi:
- variazione dei trattamenti in corso;
- utilizzo di nuovi servizi/strumenti informatici, nonché modifica di quelli esistenti.
- revisione del modello organizzativo, qualora determini significativi riflessi sui trattamenti.

La disposizione di cui all'art. 36, paragrafo 1, del Regolamento UE 2016/679 deve interpretarsi nel senso che, qualora le misure adottate non risultassero idonee ad attenuare il rischio, la Struttura competente, dopo aver predisposto la relativa richiesta di parere, deve interpellare, tramite il Responsabile della protezione dei dati, l'Autorità di controllo prima di poter procedere al trattamento.
I Dirigenti delle Strutture provinciali, nell'adempimento dell'obbligo richiamato, potranno farsi assistere, come previsto dall'articolo 28, paragrafo 3, lettera f), del Regolamento UE 2016/679, dal Responsabile del trattamento (Trentino Digitale S.p.a. o altro Responsabile esterno).

Trentino Digitale S.p.a., in qualità di Responsabile esterno dei trattamenti della Provincia, ha predisposto la metodologia per eseguire la valutazione d'impatto dei trattamenti provinciali (in collaborazione con *FBK*), quando i medesimi sono effettuati con strumenti informatici gestiti e messi a disposizione del Titolare, dalla Società; le Strutture che si avvalgono di Responsabili esterni diversi da Trentino Digitale S.p.a. e che utilizzano strumenti informatici da loro forniti e/o gestiti, sono tenute a rivolgersi agli stessi adottando, per motivi di uniformità, la medesima metodologia predisposta dalla Società di sistema (e approvata con deliberazione della Giunta provinciale n. 2004/2018).

Trentino Digitale S.p.a. è tenuta a predisporre ed aggiornare l'analisi dei rischi, correlati agli strumenti/applicativi informatici gestiti dalla Società e messi a disposizione del Titolare, nonché la metodologia della valutazione d'impatto.

La valutazione sarà effettuata, con riferimento ai trattamenti di rispettiva competenza, dai responsabili delle Strutture provinciali, tramite la compilazione degli appositi campi contenuti nel Registro delle attività di trattamento e disciplinata dalla succitata deliberazione. Per effettuare una corretta valutazione d'impatto, quindi, è propedeutico aver integralmente compilato e valutato tutti gli elementi della scheda del suddetto Registro.

4.2.6 Registro delle attività di trattamento

I Titolari e i Responsabili del trattamento sono tenuti a predisporre e conservare un Registro delle attività di trattamento i cui contenuti sono indicati dall'articolo 30 del Regolamento UE 2016/679. Si tratta di un compito fondamentale, strumentale anche per il rispetto di altri obblighi prescritti dalla normativa europea (ad es. informativa, valutazione d'impatto, ecc.), finalizzato alla realizzazione di una puntuale ricognizione dei trattamenti, che dev'essere costantemente aggiornata. Il Registro deve avere forma scritta, anche elettronica, ed essere esibito, su richiesta, all'Autorità di controllo.

La tenuta del Registro dei trattamenti non costituisce un adempimento formale, bensì è parte integrante di un sistema di corretta gestione dei dati personali.

La disposizione regolamentare ha nuovamente previsto, in altri termini, l'obbligo di redazione del c.d. "elenco dei trattamenti", introdotto, nell'ordinamento nazionale, dal D. Lgs. n. 196/2003 (Allegato B del Codice privacy) e successivamente soppresso dal D. L. n. 5/2012 (articolo 45, comma 1, lettera d)), convertito con L. n. 35/2012.

La Provincia autonoma di Trento, per effetto della deliberazione della Giunta provinciale n. 1081/2013, ha continuato a garantire la tenuta di tale elenco che, a conclusione del necessario aggiornamento finalizzato ad inserire, nel medesimo, le ulteriori informazioni richieste dalla nuova normativa europea, rappresenta il Registro delle attività di trattamento della Provincia autonoma di Trento, raggiungibile all'indirizzo: http://trattamenti.provincia.tn.it. Il Registro dei trattamenti, così come definito dal Regolamento UE 2016/679, è stato istituito con deliberazione della Giunta provinciale n. 450/2018.

Il Registro dovrà essere puntualmente compilato (inclusa la parte relativa alla valutazione d'impatto) e costantemente aggiornato, dai responsabili delle Strutture provinciali, considerata anche la sua funzione di documentazione dell'attività del Titolare.

Si rammenta, infine, come il Registro debba contenere, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento.

4.2.7 Trasferimento dei dati personali verso Paesi terzi e organizzazioni internazionali

Qualora il trattamento dei dati personali comporti il trasferimento dei medesimi verso un Paese terzo o un organizzazione internazionale al di fuori dell'Unione europea, dovrà essere applicato, scrupolosamente, il Capo V del Regolamento UE 2016/679.

Il trasferimento verso un Paese terzo caratterizzato da un livello di protezione "adeguato" (ovvero, sostanzialmente equivalente alla disciplina europea in tema di protezione dei dati) e, cioè, considerato tale da una specifica decisione della Commissione che dichiara l'adeguatezza (articolo 45 del Regolamento UE 2016/679), ovvero sulla base di "clausole contrattuali modello" debitamente adottate (articolo 46 del Regolamento UE 2016/679), o di norme vincolanti d'impresa

(articolo 47 del Regolamento UE 2016/679), può essere effettuato senza l'autorizzazione del Garante.
Tuttavia, tale autorizzazione è necessaria se il Titolare desidera utilizzare clausole contrattuali "*ad hoc*" (cioè, non adottate della Commissione europea, ovvero non adottate dal Garante ed approvate dalla Commissione), oppure accordi amministrativi stipulati tra autorità pubbliche, (modalità, queste ultime, che rappresentano una delle novità introdotte dal Regolamento UE 2016/679).

Il Regolamento UE 2016/679 ammette anche la possibilità di ricorrere a codici di condotta, oppure a schemi di certificazione, per dimostrare le "garanzie adeguate" previste dall'articolo 46. In tale specifico caso, però, i Titolari o i Responsabili del trattamento stabiliti in un Paese terzo dovranno ottemperare alle prescrizioni del codice di condotta o dello schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, assumendo, mediante un impegno contrattuale (o altro strumento che sia giuridicamente vincolante; si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2), l'obbligo di applicare le medesime adeguate garanzie, anche per quanto riguarda i diritti degli interessati.

Il Regolamento UE 2016/679 vieta trasferimenti di dati verso Titolari o Responsabili in un Paese terzo sulla base di decisioni giudiziarie od ordinanze amministrative emesse da autorità di tale Paese terzo, se non sono fondati su un accordo internazionale, quale ad esempio un trattato di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (si veda art. 48).

Qualora il trasferimento verso Paesi terzi e organismi internazionali non sia ammissibile ai sensi degli articoli 45, 46 e 47 del Regolamento UE 2016/679, potranno essere utilizzate, tuttavia, le deroghe previste per situazioni specifiche (articolo 49 del Regolamento UE 2016/679).
A tale riguardo, si rammenta che il Regolamento UE 2016/679 chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "*per importanti motivi di interesse pubblico*", in deroga al divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del Titolare o dal diritto dell'UE (si veda art. 49, paragrafo 4) e, dunque, non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

Deve, inoltre, essere evidenziato come, il primo comma, lettere a), b) e c), e il secondo comma, del paragrafo 1, dell'art. 49 del Regolamento UE 2016/679 non si applicano alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

4.2.8 Diritti dell'interessato

Ai sensi del Regolamento UE 2016/679, sono riconosciuti all'interessato i seguenti diritti: diritto di informativa (articoli 13 e 14); diritto di accesso ai propri dati (articolo 15) diritto di rettifica e integrazione dei dati (articolo 16); diritto alla cancellazione dei dati (diritto all'oblio) (articolo 17); diritto di limitazione del trattamento (articolo 18); obbligo di notifica dell'integrazione e rettifica dei dati, nonché di limitazione del trattamento (articolo 19); diritto di opposizione (articolo 21); diritto a non essere sottoposto a trattamento automatizzato (articolo 22).

Il Titolare del trattamento è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea (art. 12). Benché sia il solo Titolare a dover dare riscontro in caso di esercizio dei diritti, il Responsabile è tenuto a collaborare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e), del Regolamento UE 2016/679).
L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni nel caso di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12, paragrafo 5, del Regolamento UE 2016/679): il Titolare, in tali casi, può addebitare un contributo spese ragionevole (tenendo conto dei costi amministrativi sostenuti), oppure non fornire riscontro. E' onere del Titolare dimostrare l'infondatezza o l'eccessività della richiesta.

Il riscontro all'interessato, di regola, deve avvenire in forma scritta, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere fornito oralmente solo se così richiede l'interessato stesso, purché sia comprovata con altri mezzi l'identità del medesimo (art. 12 del Regolamento UE 2016/679). Il riscontro non dev'essere solo "intelligibile", ma anche conciso, trasparente e facilmente accessibile, oltre ad utilizzare un linguaggio semplice e chiaro.
Il Titolare ha il diritto di chiedere le informazioni necessarie a identificare l'interessato e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (art. 12 del Regolamento UE 2016/679).
Fermo restando che il riscontro all'interessato dev'essere fornito "senza ingiustificato ritardo", per tutti i diritti (escluso il diritto all'informativa) il termine massimo previsto è di 1 mese dalla richiesta, ulteriormente prorogabile di 2 mesi (quindi, per complessivi 3 mesi) in casi di particolare complessità della stessa istanza; il Titolare deve, comunque, dare un riscontro all'interessato, entro 1 mese dalla richiesta, dei motivi dell'estensione dei termini per il riscontro. Spetta al Titolare valutare la complessità del riscontro all'interessato.
In caso di diniego, il Titolare, nei medesimi termini, deve informare l'interessato della possibilità di proporre reclamo a un'Autorità di controllo o di proporre ricorso giurisdizionale.

Il diritto di accesso prevede che l'interessato possa ottenere, dal Titolare, la conferma che sia in corso, o meno, un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle informazioni indicate dall'art. 15 del Regolamento UE 2016/679.

Il Titolare, senza ledere i diritti e le libertà altrui, fornisce gratuitamente 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.
Se l'interessato presenta la richiesta mediante mezzi elettronici e salvo diversa indicazione dello stesso, le informazioni sono fornite in un formato elettronico di uso comune.

Ogni Dirigente, pertanto, sarà tenuto a fornire riscontro (avvalendosi del modello di cui alla Sezione III, della presente deliberazione), nei termini e modalità sopra descritti, alle istanze pervenute e circoscritte ai trattamenti della Struttura dallo stesso diretta, consegnando una copia dei dati personali.
Qualora, invece, la richiesta di accesso ai dati personali riguardi la Provincia, globalmente considerata, o più Strutture provinciali, il Dirigente della Struttura che riceve l'istanza sarà tenuto, nella stessa giornata di ricezione, a protocollare la richiesta ed a comunicarla a tutti i Dipartimenti provinciali e Strutture equipollenti; i Dipartimenti, a loro volta, entro 10 giorni dalla ricezione, dovranno reperire i dati personali presso le rispettive Strutture di riferimento, inviando il proprio riscontro interno (come già chiarito con la circolare prot. n. 205959 del 9/04/2018) al Direttore generale, il quale, a propria volta, fornirà il complessivo riscontro (e copia integrale dei dati raccolti) all'interessato, nel più breve tempo possibile e, comunque, non oltre i termini di legge.
Per velocizzare la ricerca dei dati personali, è opportuno che ogni Struttura proceda alla ricognizione delle banche dati utilizzate, in modo da poter disporre di un'adeguata *check list*.
In generale, per far fronte alle richieste di accesso ai dati personali e rispettare i termini stabiliti dalla normativa, è necessario che i responsabili delle Strutture provinciali si organizzino preventivamente, individuando, tra il personale assegnato, quello che dovrà effettuare, nei vari archivi, la ricerca dei dati e l'attività di estrazione, procedendo, contestualmente, alla distribuzione dei relativi compiti e fornendo adeguate istruzioni. Può essere opportuno rapportarsi anche con il Responsabile del trattamento e con la Struttura competente in materia di sicurezza informatica.

Infine, come di seguito meglio precisato, una particolare forma di accesso è prevista dall'art. 26 del Regolamento UE 2016/679, ovvero in caso di co-titolarità.

Il diritto di rettifica e integrazione prevede la possibilità, dell'interessato, di ottenere, dal Titolare, la rettifica dei dati inesatti e l'integrazione dei dati incompleti. Il termine rettifica deve intendersi,

altresì, come modifica, correzione o aggiornamento.

Il diritto di cancellazione prevede la possibilità, dell'interessato, di ottenere, dal Titolare, la cancellazione dei dati personali, quando: a) non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; c) sono stati trattati illecitamente; d) devono essere cancellati per adempiere a un obbligo giuridico previsto dal diritto dell'Unione, o dello Stato membro cui è soggetto il Titolare; (e) per revoca del consenso, laddove non sussista altra base legittima per il trattamento).
Le regole sopracitate non si applicano quando il trattamento è necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo giuridico 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 a quanto prescrivono l'articolo 9, paragrafo 2, lettere h) e i), e l'articolo 9, paragrafo 3, del Regolamento UE 2016/679; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del Regolamento UE 2016/679, nella misura in cui il diritto di cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Il Garante, con il provvedimento n. 243/2014, ha definito alcune regole per garantire il diritto all'oblio degli interessati, nei casi in cui la norma non preveda un termine che delimiti gli effetti della pubblicazione.
A tal proposito, l'Autorità di controllo ha evidenziato la necessità di prevedere meccanismi (e/o procedure) che impediscano la indiscriminata permanenza, dei vari atti (e, di conseguenza, delle informazioni e dei dati in essi contenuti), sui siti istituzionali dei soggetti pubblici.
Il Garante, nel provvedimento citato, ha individuato, in modo non esaustivo, alcune modalità di trattamento ritenute idonee a limitare l'ingiustificata esposizione pubblica dei dati:
- privilegiare motori di ricerca interni al sito istituzionale dell'Amministrazione, in modo da garantire una selezione degli accessi;
- stabilire i tempi di permanenza degli atti sul sito. Tale durata, nei casi in cui non sia già prevista dalla legge, potrebbe essere garantita 1) dalla rimozione, dal sito *web*, dopo il decorso del periodo di tempo stabilito per il raggiungimento degli scopi di pubblicazione; 2) dalla permanenza dei documenti, nel sito *web*, ma oscurando gli elementi di identificazione dell'interessato;
- utilizzare *software* o programmi automatici, per evitare duplicazioni massive di *files* (e, dunque, di dati) e anomale riproduzioni;
- adottare misure per ridurre, o eliminare, il rischio di cancellazioni, modifiche, alterazioni o decontestualizzazioni, al fine di garantire che i dati diffusi siano, in ogni caso, esatti ed aggiornati.

Il diritto di limitazione prevede la possibilità di ottenere, dal Titolare, la limitazione del trattamento per i seguenti motivi: a) perché si ritiene che il dato o i dati non siano esatti e fino al momento in cui verranno rettificati; b) perché, pur ritenendo il trattamento dei dati illecito, l'interessato è contrario alla cancellazione dei dati; c) perché i dati, pur non essendo più necessari al Titolare, servono all'interessato per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria; d) perché l'interessato si è opposto al trattamento dei propri dati ed è in attesa della verifica in merito alla prevalenza dei suoi legittimi motivi rispetto a quelli del Titolare.
Se il trattamento è limitato, i dati personali sono trattati, salvo che per la conservazione, soltanto 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 di uno Stato membro. L'interessato che ha ottenuto la limitazione del trattamento è informato, dal Titolare del trattamento, prima che detta limitazione sia revocata.

Ai sensi dell'art. 19 del Regolamento UE 2016/679, il Titolare è obbligato ad informare gli altri Titolari delle rettifiche, o cancellazioni, o limitazioni del trattamento effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare comunica all'interessato i nominativi di tali destinatari, qualora lo stesso lo richieda.

Il diritto di opposizione prevede la possibilità che l'interessato possa opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare (v. art. 6.1, lett. e), del Regolamento UE 2016/679), compresa la profilazione effettuata avvalendosi di tale base legittima.
Il Titolare, salvo che dimostri l'esistenza di motivi legittimi cogenti che prevalgano sugli interessi, sui diritti e sulle libertà dell'interessato, oppure salvo che dimostri che il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, si astiene dal trattare ulteriormente i dati personali.
Qualora i dati personali siano trattati a fini di ricerca scientifica, o storica, o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Ai sensi dell'art. 22 del Regolamento UE 2016/679, 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 riguardino o che incida in modo analogo significativamente sulla sua persona.
Tale diritto 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 il Titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento, 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).
Nel caso di cui alla precedente lett. a) (o, alla lett. c)), il Titolare adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, quantomeno, in particolare, il diritto di quest'ultimo di ottenere l'intervento umano da parte del Titolare stesso, di esprimere la propria opinione e di contestare la decisione.
Tali decisioni, a meno che non sia applicabile l'articolo 9, paragrafo 2, lettera g) (motivi di rilevante interesse pubblico esplicitamente previsto da norma di legge o di regolamento) e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, non possono avere ad oggetto categorie particolari di dati personali.

Ulteriori diritti sono altresì previsti dagli artt. 34 e 11.2 del Regolamento UE 2016/679.

Ai sensi dell'art. 23 del Regolamento UE 2016/679, "*il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare*" taluni valori fondamentali indicati dallo stesso articolo (a cui, pertanto, si rinvia).
Di conseguenza, in attuazione parziale (ovvero, escludendo forme di limitazione dei diritti di cui agli artt. 12, 13 e 14 del Regolamento UE 2016/679) di tale disposizione normativa europea, l'art. 2-*undecies* del D. Lgs. n. 196/2003 stabilisce che "*i diritti di cui agli articoli* ***da 15 a 22*** *del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto*" ad alcuni valori fondamentali (tra cui, particolari interessi e diritti di riservatezza) previsti dallo stesso articolo (al quale, pertanto, si rinvia).

Ai sensi del comma 3 del medesimo art. 2-*undecies*, "*l'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso* ***con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione****, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi*" (cioè, i valori fondamentali per cui è prevista la limitazione stessa dei diritti dell'interessato). Nella succitata comunicazione all'interessato, il Titolare lo informa della facoltà di esercitare i propri diritti, per mezzo del Garante, con le modalità di cui all'art. 160 del D. Lgs. n. 196/2003.

Si rammenta, inoltre, che l'art. 2-*terdecies* del D. Lgs. n. 196/2003 prevede che: "***I diritti*** *di cui agli articoli* ***da 15 a 22 del Regolamento*** *riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione*".

4.2.9 Regolamento per il trattamento dei dati *ex* artt. 9 e 10 del Regolamento UE 2016/679

L'art. 2-*sexies* del D. Lgs n. 196/2003 prevede, al comma 1, che "*I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento... sono ammessi quando siano previsti... nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento* ***che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili, e il motivo di interesse pubblico rilevante nonché le misure appropriate e specifiche*** *per tutelare i diritti fondamentali e gli interessi dell'interessato*".
In buona sostanza, quindi, la citata norma, introdotta dal recente D. Lgs. n. 101/2018, ribadisce, come in passato, che i soggetti pubblici, per poter trattare quelli che una volta erano qualificati "dati sensibili" (ora dati "particolari"), necessitano di norme di legge, o di regolamento, caratterizzate da un contenuto specifico; l'articolo 2-*octies* del D. Lgs n. 196/2003 estende la disciplina prevista dall'art. 2-*sexies* ai dati che erano denominati "dati giudiziari" (per la nuova normativa, dati relativi a "condanne penali e reati").

L'elemento innovativo richiesto dal Codice, così come armonizzato, e che costituisce ulteriore oggetto della norma di legge o di regolamento, è rappresentato, in aggiunta alla tipologia dei dati da trattare, alle operazioni di trattamento eseguibili ed alle finalità di rilevante interesse pubblico del trattamento, dalla indicazione delle specifiche ed appropriate misure, tecniche ed organizzative, che il Titolare (o il Responsabile) del trattamento ritiene di adottare a tutela dell'interessato.

La Provincia, in virtù della previgente normativa, ha approvato, con decreto del Presidente n. 27-129/Leg dell'8/10/2013, la nuova versione del "Regolamento per il trattamento dei dati sensibili e giudiziari", ancora oggi in vigore; in virtù di quanto previsto dall'attuale normativa in tema di protezione dei dati personali, quindi, sarà necessario provvedere alle opportune modifiche/integrazioni. Relativamente alle misure tecnico-informatiche per il trattamento di tali tipologie di dati, pertanto, la società Trentino Digitale S.p.a. è tenuta ad adottare ed aggiornare le suddette misure, trasmettendo il relativo elenco all'Ufficio organizzazione e gestione della privacy e alla Struttura competente in materia di sicurezza informatica, per la loro valutazione e successivo inserimento nel D.P.P. n. 27-129/Leg..

Ferma restando la possibile adozione di ulteriori e più elevate misure di sicurezza tecniche ed organizzative per il trattamento di tali categorie di dati, sarà compito del Dirigente inviare, ai Responsabili esterni (diversi da Trentino Digitale S.p.a) della Struttura di cui è responsabile, le misure previste nel D.P.P. n. 27-129/Leg. (eventualmente, integrandole con quelle ulteriormente adottate), imponendone, agli stessi, il rispetto. *Pro futuro*, tali specifiche misure potranno essere direttamente incluse (anche come allegato) nel contratto di nomina a Responsabile esterno.

4.3 Diffusione di dati personali tramite pubblicazione sul B.U.R. e sul sito istituzionale della Provincia

La pubblicazione sul B.U.R. e sul sito istituzionale della Provincia, di atti contenenti dati personali, concretizza un'ipotesi di diffusione degli stessi. Tale pubblicazione è in linea con quanto disposto dall'art. 6 del Regolamento UE 2016/679 e dal comma 3, dell'art. 2-*ter*, del D. Lgs. n. 196/2003, essendo espressamente prevista dalla legge provinciale n. 23 del 30 novembre 1992 (art. 31, commi 1 e 7) e dalla legge provinciale n. 16 del 27 luglio 2012 (art. 9).

Nell'applicare le disposizioni che stabiliscono forme e modalità di pubblicazione, la Struttura redigente deve, comunque, effettuare una verifica sulla pertinenza e non eccedenza dei dati personali contenuti negli atti oggetto di diffusione (e sull'indispensabilità, nel caso di dati di cui agli artt. 9 e 10 del Regolamento UE 2016/679), anche quando di tale atto è prevista la pubblicazione integrale (v. anche il Provvedimento del Garante n. 243 del 2014 "*Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*"), avendo cura di evitare la diffusione di dati personali non necessari alla finalità di trasparenza dell'azione amministrativa, sottesa alla pubblicazione (possibili soluzioni, che non ne escludono di ulteriori, sono quelle consistenti nell'inserimento dei dati personali non strettamente pertinenti al provvedimento, ma necessari per adempimenti successivi – quali, ad es., codice fiscale, coordinate bancarie, conto corrente postale del beneficiario e simili – in un documento allegato, che non viene pubblicato, oppure nella predisposizione, ai fini della pubblicazione dell'atto, di un testo nel quale tali dati siano omessi/oscurati).

Non sono pubblicabili, in forma integrale, ma possono costituire oggetto di "pubblicazione per estremi", gli atti "riservati" e cioè quelli contenenti informazioni che, pur costituendo dati personali, sono comprese nelle fattispecie indicate negli articoli 31, comma 2, 32, comma 4, e 32-*bis*, commi 1 e 2, della legge provinciale n. 23 del 30 novembre 1992 (e relativo regolamento di attuazione), nonché nell'articolo 24, commi 1 e 6, della legge n. 241/1990 (e D.P.R. n. 352/1992).

Non possono essere diffusi, come anzidetto, i dati relativi alla salute, quelli genetici e biometrici (art. 2-*septies*, comma 8, del D. Lgs. n. 196/2003), nonché – in caso di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici – i dati identificativi delle persone fisiche beneficiarie dei succitati provvedimenti, "*qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati*" (art. 26, comma 4, del D. Lgs. n. 33/2013).

4.4 Rapporti tra normativa sulla protezione dei dati personali, diritti d'accesso e trasparenza amministrativa

Ai sensi del considerando n. 154 del Regolamento UE 2016/679 "*Il presente regolamento ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali. L'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico. I dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti. Tali disposizioni legislative dovrebbero conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali e possono quindi prevedere la necessaria conciliazione con il diritto alla protezione dei dati personali, in conformità del presente regolamento*". L'art. 86 del Regolamento UE 2016/679 stabilisce che "*I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo*

conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento".

4.4.1 Accesso ai documenti amministrativi

La legge provinciale 30 novembre 1992, n. 23 "*Principi per la democratizzazione, la semplificazione e la partecipazione all'azione amministrativa provinciale e norme in materia di procedimento amministrativo*", in attuazione dello Statuto e del principio di massima trasparenza e pubblicità dell'azione amministrativa, prevede, al Capo VI, specifiche disposizioni in merito all'accesso ai documenti amministrativi della Provincia, raccordandosi sia con la legge n. 241/1990, che con il D. Lgs. n. 196/2003.

Il diritto di accesso previsto dalla L.P. n. 23/1992 (e dalla L. n. 241/1990):
• assicura la pubblicità dell'attività amministrativa;
• riguarda esclusivamente i documenti amministrativi;
• prevale, rispetto al diritto alla protezione dei dati personali, nel caso in cui sia strumentale alla cura o tutela di interessi giuridici.

Il diritto alla protezione dei dati personali previsto dal D. Lgs. n. 196/2003:
• garantisce il rispetto dei diritti, delle libertà fondamentali e della dignità dell'individuo;
• riguarda il dato personale;
• recede, nel caso in cui si debba garantire l'accesso per la cura o tutela di interessi giuridici.

Entrambi i diritti (accesso/protezione dei dati personali) godono di pari rango e, solo apparentemente, sono tra loro in contrasto poiché la normativa in materia di protezione dei dati personali si pone come fattore delimitativo, sotto il profilo delle modalità tecniche di esercizio, ma non preclusivo dell'accesso.
L'articolo 59 del D. Lgs. n. 196/2003 stabilisce che i presupposti, le modalità e i limiti del diritto di accesso restano disciplinati dalla Legge n. 241/1990 e s.m.i.; l'art. 2-*sexies* del D. Lgs. n. 196/2003 conferma che il diritto di accesso deve ritenersi di rilevante interesse pubblico.

Il diritto d'accesso ai documenti amministrativi è consentito solo a coloro che, previa richiesta motivata, vantino un interesse diretto, attuale e concreto.

Fermi restando gli artt. 32 e 32-*bis* della legge provinciale n. 23/1992, nonché gli artt. 22 (principi per l'accesso) e 24 (esclusione dell'accesso) della L. n. 241/1990, la disciplina da applicare, con riferimento ai singoli casi, si distingue in base al tipo di dati personali contenuti nel documento oggetto della richiesta di accesso:

- documento contenente i c.d. dati comuni: si applica l'art. 32-*bis*, comma 2, della legge provinciale n. 23/1992 (e l'art. 24, comma 7, della L. n. 241/1990), in virtù dei quali deve comunque essere garantito l'accesso ai documenti la cui conoscenza sia necessaria per curare o difendere i propri interessi giuridici;

- documento contenente categorie particolari di dati (*ex* dati sensibili) e dati relativi a condanne penali e reati (*ex* dati giudiziari): si applica l'art. 32-*bis*, comma 2, della legge provinciale n. 23/1992 (e l'art. 24, comma 7, della L. n. 241/1990), in base al quale l'accesso è consentito nei limiti in cui sia strettamente indispensabile per curare o difendere i propri interessi giuridici. La richiesta di accesso deve contenere la motivazione dell'indispensabilità;

- documento contenente dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona (*ex "*dati supersensibili"): si applica l'art. 60 del D. Lgs. n. 196/2003 (e l'art. 32-*bis*, comma 2, della legge provinciale n. 23/1992) in base al quale "*il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero*

consiste in un diritto della personalità o in un altro diritto o libertà fondamentale". La norma pone, dunque, in capo alla P.A. l'onere di un doppio giudizio discrezionale relativo sia all'indispensabilità dell'accesso che alla comparazione degli interessi da tutelare.

Il Garante ha stabilito che, nel valutare il "rango" del diritto di un terzo, si deve utilizzare come parametro di raffronto non il "diritto di azione e difesa", che pure è costituzionalmente garantito, quanto il diritto sottostante che il terzo intende tutelare in giudizio, sulla base del documento in relazione al quale promuove l'accesso.

4.4.2 Diritto di accesso dei Consiglieri provinciali

I Consiglieri provinciali hanno diritto di ottenere tutte le notizie e le informazioni (articolo 147 della Deliberazione del Consiglio provinciale n. 3/1991), in possesso degli uffici provinciali, che siano utili all'espletamento del proprio mandato.
La concreta individuazione, da parte degli uffici, delle notizie e delle informazioni che possono essere comunicate, quindi, deve tener conto di tutto ciò che può essere funzionale allo svolgimento del mandato stesso e, pertanto, consentire ai Consiglieri di valutare con piena cognizione di causa l'operato dell'Amministrazione, di esprimere un voto consapevole sulle questioni sottoposte all'organo consiliare e di promuovere le iniziative di competenza.
Essendo il Consigliere tenuto al segreto (art. 43 del D. Lgs. n. 267/2000), il relativo accesso non è sottoposto ad alcun bilanciamento con la specifica natura dei dati contenuti nella notizia/informazione richiesta, ma soltanto a un giudizio di minimizzazione dei dati personali da sottoporre all'accesso; in altri termini, l'Amministrazione non dovrà comunicare dati che non siano strettamente pertinenti e limitati rispetto all'espletamento del mandato.

4.4.3 Trasparenza e diritto di accesso civico "generalizzato"

La protezione dei dati personali è materia che impatta su un altro rilevante ambito d'intervento della Provincia: la trasparenza amministrativa (disciplinata dal D. Lgs. n. 33/2013 e dalla L.P. n. 4/2014).
L'art. 59 del D. Lgs. n. 196/2003 stabilisce che "*I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33*".
Il Decreto Legislativo n. 33/2013 prevede ipotesi nelle quali è obbligatorio pubblicare dati personali, informazioni e documenti, stabilendo, inoltre, che possono anche essere pubblicati dati personali, informazioni e documenti non soggetti a tale obbligo, purché si proceda all'anonimizzazione dei dati personali eventualmente presenti (articolo 7-*bis*, comma 3, del D. Lgs. n. 33/2013).

L'articolo 5 (Accesso civico a dati e documenti) del D. Lgs. n. 33/2013 stabilisce, al comma 2, che "*chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni,* ***ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto****, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis*".

L'articolo 5-*bis* (Esclusioni e limiti all'accesso civico) del D. Lgs. n. 33/2013, a propria volta, contempla, tra i motivi che possono determinare la limitazione dell'accesso civico, "*la protezione dei dati personali, in conformità con la disciplina legislativa in materia*" (comma 2, lettera a)).

Conseguentemente, sarà compito di ogni singola Struttura provinciale effettuare il bilanciamento tra le esigenze relative alla trasparenza in rapporto a quelle connesse con la protezione dei dati personali, tenendo presente che "*Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione*" e fermo restando il divieto di diffusione

dei "*dati idonei a rivelare lo stato di salute e la vita sessuale*" (art. 7-*bis*, commi 4 e 6, del D. Lgs. n. 33/2013).

5. DISPOSIZIONI ORGANIZZATIVE

5.1 I ruoli nel sistema di gestione dei dati personali

L'applicazione delle norme in materia di protezione dei dati personali comporta l'attribuzione di compiti e responsabilità in capo alle seguenti figure:

- Titolare del trattamento (art. 4, n. 7, del Regolamento UE 2016/679);
- Responsabile del trattamento (art. 4, n. 8, del Regolamento UE 2016/679);
- Persone che agiscono sotto l'autorità diretta del Titolare o del Responsabile del trattamento (artt. 4, n. 10, 29 e 32 del Regolamento UE 2016/679; art. 2-*quaterdecies* del D. Lgs. n. 196/2003).

Il Garante ha affermato che "*il Regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento negli stessi termini di cui alla Direttiva 95/46 CE e, quindi, al Codice italiano*". In particolare, poi, l'Autorità ha valutato le disposizioni del D. Lgs. n. 196/2003 in tema di "Incaricati del trattamento" "*pienamente compatibili con la struttura e filosofia del regolamento*", ritenendo "*opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento*".

L'art. 2-*quaterdecies* del D. Lgs. n. 196/2003 stabilisce espressamente che "*il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

5.1.1 Titolare e Responsabile del trattamento

Il Titolare, secondo la definizione del Regolamento UE 2016/679, è il soggetto (persona fisica, giuridica, pubblica amministrazione, servizio o altro organismo) che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento (art. 4, n. 7).

La Giunta provinciale, già con le deliberazioni nn. 3216 del 23 dicembre 2002 e 1081 del 7 giugno 2013 (sostituita dalla presente), ha dato atto che la Provincia autonoma di Trento (come persona giuridica) è Titolare del trattamento dei dati personali strumentali all'esercizio delle funzioni istituzionali attribuite dall'ordinamento.

Nell'esercizio delle funzioni di Titolare, la Provincia opererà, in concreto, attraverso gli organi (Presidente e Giunta provinciale) ed i soggetti di volta in volta competenti in base all'ordinamento provinciale.

Spetta al Presidente della Provincia

- rappresentare il Titolare.

Spetta alla Giunta provinciale:

- la deliberazione del regolamento in tema di trattamento dei dati di cui agli artt. 9 e 10 del Regolamento UE 2016/679, nonché 2-*sexies*, 2-*septies* e 2-*octies* del D. Lgs. n. 196/2003;
- la definizione dell'impianto organizzativo provinciale in materia di protezione dei dati personali;

- l'adozione delle decisioni in ordine alle finalità e ai mezzi del trattamento, avvalendosi, nell'ambito delle relative competenze, dei responsabili delle Strutture provinciali (Preposti al trattamento);
- l'elaborazione delle istruzioni da impartire a coloro che agiscono sotto l'autorità dell'organo di governo provinciale;
- la determinazione delle misure tecniche ed organizzative adeguate a garantire un livello di sicurezza dei trattamenti conforme a quanto stabilito dall'articolo 32 del Regolamento UE 2016/679;
- deliberare la metodologia sulla base della quale effettuare la valutazione dei rischi/d'impatto del trattamento;
- la pianificazione degli interventi di adeguamento;
- la vigilanza (controllo di primo livello), anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, e sul rispetto delle proprie istruzioni. Tali verifiche saranno effettuate tramite i Dirigenti, nell'ambito dell'attività connessa all'esercizio delle funzioni di direzione, coordinamento e controllo delle Strutture dirette, e, in relazione ai controlli sull'applicazione delle misure di sicurezza informatica previste nella Sezione II, tramite il responsabile della Struttura competente in materia di sicurezza informatica, che potrà avvalersi anche di soggetti esterni;
- la nomina, attraverso l'apposito contratto (o clausola), dei Responsabili esterni del trattamento (che verrà effettuata, per conto del Titolare, dai Dirigenti delle rispettive Strutture), nonché dei Preposti al trattamento;
- l'autorizzazione al trattamento del personale provinciale e di eventuali soggetti esterni, nominati Addetti al trattamento (per conto del Titolare, da parte dei Dirigenti delle rispettive Strutture);
- la nomina del Responsabile della protezione dei dati (DPO);
- l'adozione del Registro dei trattamenti.

Laddove la Provincia si avvalga della collaborazione di soggetti esterni (sulla base di concessioni, appalti, contratti, convenzioni, consulenze, collaborazioni, tirocini, ecc.), questi ultimi, nell'ambito del correlativo rapporto, possono spesso venire a conoscenza di dati personali di cui la Provincia è Titolare.
Per gestire tale situazione, è necessario che, nell'ambito delle convenzioni o degli atti che disciplinano il rapporto di collaborazione, venga individuato, in relazione al trattamento dei dati, il ruolo più idoneo di cui dovrà essere investito il soggetto esterno. Quest'ultimo può essere qualificato:

- Titolare (autonomo) oppure Co-titolare;
- Responsabile del trattamento;
- Autorizzato al trattamento.

Se il collaboratore esterno, nell'ambito del rapporto contrattuale/convenzionale, vanta un'ampia autonomia in ordine al trattamento dei dati personali e, cioè, tratta i dati personali (conosciuti nel corso del rapporto stesso e di cui la Provincia è Titolare) per finalità proprie (ovvero, distinte rispetto a quelle della Provincia), oltre che con mezzi autonomamente determinati, la corretta qualificazione dovrebbe essere quella di Titolare (autonomo) del trattamento. Di conseguenza, la trasmissione di dati personali, dalla Provincia al soggetto esterno, anche nella forma dell'accesso alle proprie banche dati, configura una "comunicazione" di dati ed è legittimata solo nel rispetto dei presupposti di cui agli articoli 2-*ter*, 2-*sexies* e 2-*octies* del D. Lgs. n. 196/2003, come precedentemente descritte.
In tale ipotesi, inoltre, il soggetto esterno deve determinare le misure tecniche ed organizzative, nonché le cautele previste dalla normativa vigente.

Resta inteso che ogni ente strumentale di cui all'art. 33 della L.P. n. 3/2006, relativamente al trattamento dei dati trattati per proprie finalità e con strumenti autonomamente determinati (fatti salvi eventuali casi di contitolarità) si configura come Titolare del trattamento, con ogni relativa conseguenza anche in merito all'autonoma predisposizione delle informative (*ex* artt. 13 e 14 del Regolamento UE 2016/679), all'ulteriore modulistica e al Registro dei trattamenti (*ex* art. 30 del Regolamento UE 2016/679), oltre che all'adozione delle misure di sicurezza (*ex* art. 32 del Regolamento UE 2016/679), all'effettuazione della valutazione di impatto (*ex* artt. 35-36 del Regolamento UE 2016/679), alla notifica/comunicazione dei *data breach* e relativa conservazione della documentazione (*ex* artt. 33-34 del Regolamento UE 2016/679), nonché all'individuazione e nomina del proprio Responsabile della protezione dei dati (DPO) (*ex* artt. 37-38-39 del Regolamento UE 2016/679). Tutto ciò, non esclude la possibilità che, in forza del contenuto dello specifico contratto di servizio, l'ente strumentale possa altresì assumere il ruolo di Responsabile esterno della Provincia.

Ulteriore fattispecie sarebbe configurabile allorché il soggetto esterno (specie se rappresentato da un ente pubblico) condividesse finalità e mezzi del trattamento (ad esempio, nell'ipotesi di piattaforma comune per il trattamento dei dati) con la Provincia: tale situazione potrebbe essere riconducibile ad una situazione di contitolarità.
L'articolo 26, paragrafo 1, del Regolamento UE 2016/679 stabilisce che "*Allorché due o più titolari del trattamento* ***determinano congiuntamente le finalità e i mezzi*** *del trattamento,* ***essi sono contitolari del trattamento***"; i Co-Titolari (o Contitolari) sono tenuti a disciplinare il loro rapporto mediante un accordo, tramite il quale determinano i rispettivi obblighi e responsabilità. Spetta ai Dirigenti provinciali, con riferimento ai trattamenti di propria competenza, stipulare gli eventuali accordi di contitolarità (il cui modello è allegato al presente provvedimento) e darne adeguata informativa, agli interessati, secondo quanto previsto dall'art. 26 predetto. Nel rispetto dell'art. 26.2, è allegato alla presente deliberazione anche uno specifico modello di riscontro per l'interessato.

Nella maggior parte dei casi, tuttavia, è ravvisabile l'opportunità che la Provincia conservi il potere di decidere in ordine alle finalità e ai mezzi del trattamento; in tali ipotesi, si dovrà procedere – con gli adeguati strumenti giuridici – all'individuazione/nomina, in forma espressa, del soggetto esterno quale Responsabile del trattamento o Autorizzato al trattamento (in relazione al maggiore, o minore, ambito di intervento sui dati e alle correlative responsabilità che al medesimo vengono attribuite), impartendo, al medesimo, le imprescindibili istruzioni/direttive. La fattispecie del Responsabile esterno, in particolare, potrebbe realizzarsi allorché, pur nell'ambito di una delega conferita al soggetto esterno (che, quindi, non si limita ad essere un mero esecutore materiale/operativo), la Provincia non si spossessasse integralmente dei poteri e delle funzioni (come nel caso di vero e proprio trasferimento delle competenze), mantenendo un potere di indirizzo mediante la fissazione dei criteri e/o dei principi generali, un potere di controllo/verifica sul rispetto delle direttive, nonché un potere decisionale sull'operatività del soggetto esterno. Pertanto, sebbene il soggetto esterno possa, talvolta, anche apparire come diretto ed unico interlocutore dell'interessato, lo stesso agisce in realtà per conto del Titolare, vero *dominus* del trattamento dei dati personali.
Il Regolamento UE 2016/679 (articolo 4, paragrafo 8), quindi, definisce 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***".

Il Titolare è tenuto a ricorrere a Responsabili del trattamento "*che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*" (articolo 28, paragrafo 1, del Regolamento UE 2016/679).

Il contratto (o altro atto giuridico che vincoli il Responsabile), che regola il rapporto tra il Titolare ed il Responsabile, deve necessariamente disciplinare la materia oggetto di affidamento, natura, finalità e durata del trattamento, tipo di dati personali e categorie di interessati, nonché i rispettivi obblighi e responsabilità, dovendo altresì contenere quanto prescritto dall'articolo 28, paragrafi 3 e 4, del Regolamento UE 2016/679.

Qualora ritenuto opportuno, il contratto di nomina del Responsabile del trattamento potrà costituire, per i rapporti in corso, un allegato del contratto (o convenzione/accordo/ecc.) principale di affidamento del servizio; per i nuovi rapporti, il contratto di nomina del Responsabile esterno potrà anche costituire una specifica clausola del contratto principale. Si evidenzia che, nel rispetto dei principi di cui agli artt. 5.2, 32 e 35 del Regolamento UE 2016/679, il Dirigente dovrà valutare se, in relazione ai rischi derivanti dagli specifici dati trattati e dalle operazioni compiute, indicare particolari misure di sicurezza che ritiene "idonee" e che lo stesso Responsabile esterno è tenuto ad adottare.

Il Responsabile del trattamento, ai sensi dell'art. 30, paragrafo 2, del Regolamento UE 2016/679 deve altresì predisporre un Registro dei trattamenti effettuati per conto del Titolare (uno per ciascun Titolare).

Nei casi in cui il soggetto esterno sia qualificabile come "Autorizzato al trattamento", o "Responsabile del trattamento", la trasmissione dei dati personali, dalla Provincia al soggetto stesso, non costituisca una "comunicazione", dal momento che il collaboratore è considerato alla stregua di un'articolazione organizzativa del Titolare (e, quindi, soggetto indistinto rispetto a quest'ultimo).

Presso la bacheca (o il sito *web* della Struttura provinciale), è conservato l'elenco dei Responsabili esterni del trattamento della Struttura stessa.

I Dirigenti provinciali, ai quali è attribuito sulla base dell'ordinamento vigente (art. 10, commi 1 e 3, D.P.G.P. n. 6-78/Leg.), il potere di stipulare i contratti di affidamento di servizi per conto della Provincia, provvedono direttamente alla designazione del Responsabile esterno, o dell'Autorizzato al trattamento, in conformità a quanto richiesto dagli articoli 28, 29 e 32 del Regolamento UE 2016/679, attraverso la stipula/sottoscrizione, rispettivamente, dello specifico contratto di nomina, o dell'atto di autorizzazione al trattamento (di cui alla successiva Sezione III).

5.1.2 Preposto al trattamento

Considerato il quadro normativo sopra illustrato, emerge la necessità di disciplinare l'organizzazione interna dei trattamenti del Titolare, adeguando l'impianto organizzativo, adottato antecedentemente al 25 maggio 2018, ai principi del Regolamento UE 2016/679.
Constatata la complessità (per dimensioni e funzioni) della Provincia, si ritiene necessario individuare, tra coloro che agiscono sotto la diretta autorità del Titolare del trattamento, figure apicali deputate al governo ed alla gestione dei trattamenti.

I soggetti attraverso i quali vengono esercitate le funzioni dell'amministrazione provinciale (L.P. n. 7/1997, articoli 2, comma 1, 3, comma 1, 16 e 17) sono i Dirigenti delle varie articolazioni organizzative che, tra l'altro, assumono la responsabilità, in via esclusiva, delle funzioni loro assegnate; appurato che, per l'esercizio delle funzioni istituzionali (e dei relativi compiti) è indispensabile procedere al trattamento dei dati personali connessi alle medesime, tra gli obblighi dei Dirigenti provinciali deve ritenersi incluso quello della gestione e responsabilità dei trattamenti riconducibili alle competenze delle Strutture dirette.

In tal senso, i Dirigenti provinciali sono qualificati come "Preposti al trattamento" (di seguito, per brevità, il "Preposto").

Con la presente deliberazione, i Dirigenti provinciali sono autorizzati a gestire i trattamenti di dati personali connessi alle materie di rispettiva competenza e alle funzioni di gestione amministrativa, finanziaria e tecnica.
Pertanto, il Dirigente, in qualità di Preposto:
- si attiene alle istruzioni impartite dal Titolare;
- non svolge meri compiti esecutivi (come quelli spettanti agli Addetti al trattamento), ma traduce in istruzioni operative le scelte strategiche e le direttive generali impartite dal Titolare, puntualizzandole e adattandole agli specifici contesti lavorativi e di trattamento.

La funzione di Preposto non può essere delegata in nessun caso. Inoltre, così come stabilito dal D.P.C.M. 3/12/2013, il Preposto, se necessario, si interfaccia con il Responsabile della conservazione digitale.

Istruzioni del Titolare - Adempimenti del Preposto al trattamento in materia di misure di sicurezza

Il Preposto, in via generale, provvede principalmente ai seguenti adempimenti (declinati in modo non esaustivo):

A) Verifica dei trattamenti

trattare i dati personali nel rispetto delle vigenti norme e delle disposizioni impartite dal Titolare.
Pertanto, per qualsiasi trattamento, il Preposto verifica che i dati siano:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato *(«liceità, correttezza e trasparenza»*);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità; («*limitazione della finalità*»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («*minimizzazione dei dati*»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («*esattezza*»);
e) conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («*limitazione della conservazione*»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative idonee, da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentale («*integrità e riservatezza*»).

Ogni Preposto deve accertare, periodicamente, la sussistenza di tali requisiti, nelle diverse fasi del trattamento, rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.
Qualora l'interessato rilasci, spontaneamente, dati eccedenti rispetto a quelli strettamente indispensabili per lo svolgimento delle attività di competenza provinciale, tali dati devono essere cancellati.
Tra i principi che caratterizzano un legittimo trattamento, infatti, assumono particolare rilevanza quelli della pertinenza e non eccedenza delle informazioni rispetto alle finalità per le quali i dati personali vengono raccolti e trattati. Il trattamento di alcuni dati, ad esempio, può essere necessario per la fase istruttoria del procedimento amministrativo, ma la loro conoscenza può risultare ingiustificata da parte di soggetti diversi da quelli incaricati di svolgere specifici compiti; la verifica del corretto trattamento comporta, se necessario, la revisione delle modalità organizzative degli uffici e l'adozione di conseguenti ed idonee misure di sicurezza.
Più specificamente, il Preposto, con riferimento ai trattamenti di competenza della Struttura di appartenenza, deve:

- verificare che i trattamenti in corso, o da attivare, siano rispondenti a quanto disposto dalla vigente normativa: il trattamento, ove difforme dalle norme, deve essere adeguato o cessare; in particolare, è indispensabile evitare l'ingiustificata e prolungata permanenza dei dati personali sui siti istituzionali della Provincia;
- in caso di comunicazione di dati, diversi da quelli "particolari" e/o relativi a "condanne penali e reati", a soggetti che li utilizzino per lo svolgimento di compiti di interesse pubblico e funzioni istituzionali, effettuare (qualora non sussista una norma di legge o di regolamento) la comunicazione al Garante di cui all'art. 2-*ter*, comma 2, del D. Lgs. n. 196/2003;
- rispettare, nell'ipotesi di trasferimento dei dati fuori dall'Unione europea, le prescrizioni previste dagli artt. 44 e seguenti del Regolamento UE 2016/679;
- provvedere al censimento dei trattamenti della Struttura di appartenenza, procedere all'inserimento dei trattamenti nel Registro elettronico (reperibile all'indirizzo *web* http://trattamenti.provincia.tn.it) e verificare che lo stesso Registro sia costantemente aggiornato;
- provvedere, tramite la procedura contenuta nel Registro elettronico dei trattamenti, ad effettuare la valutazione d'impatto (articolo 35 del Regolamento UE 2016/679);
- consultare il Garante nel caso in cui, a seguito della valutazione d'impatto, i trattamenti continuino a presentare un rischio elevato e misure di sicurezza inadeguate (articolo 36 del Regolamento UE 2016/679);
- consultare il Garante in caso di elaborazione di un testo normativo (art. 36.4 del Regolamento UE 2016/679), predisponendo lo stesso nel rispetto dei principi di cui agli artt. 5, 25 e 32 del Regolamento UE 2016/679, nonché di quanto previsto dal D. Lgs. n. 196/2003;
- predisporre l'informativa di cui agli articoli 13 e 14 del Regolamento UE 2016/679 e verificare che sia chiara, intelligibile, completa ed effettivamente portata a conoscenza degli interessati, secondo il principio di *accountability* in materia di trasparenza;
- adattare la modulistica alle specifiche esigenze della Struttura di riferimento;
- qualora la violazione dei dati personali (articolo 33 del Regolamento UE 2016/679) riguardasse sistemi informativi/applicativi "interni", cioè gestiti in autonomia dalla singola Struttura provinciale, o fosse connessa all'organizzazione della medesima Struttura, ottemperare alla seguente procedura: entro 48 ore dalla scoperta della violazione, verificare (eventualmente, con l'ausilio del Responsabile esterno) se la stessa debba essere notificata al Garante e, in caso affermativo, compilare il modello allegato alla presente deliberazione e trasmettere il relativo modello (debitamente compilato) all'Ufficio Organizzazione e gestione della privacy (che, provvederà all'inoltro della comunicazione al Garante entro le successive 24 ore);
- nel caso di cui al precedente alinea, ottemperare all'ulteriore seguente procedura: verificare, in caso di violazione di dati personali (art. 34 del Regolamento UE 2016/679), se sussistano le condizioni per la comunicazione agli interessati coinvolti dalla violazione e, in caso di esito positivo, provvedere direttamente alla comunicazione (mediante il modello di cui alla Sezione III) senza ingiustificato ritardo, il che significa prima possibile e, comunque, entro 72 ore dalla scoperta della violazione;
- nell'ipotesi in cui il responsabile della Struttura provinciale accertasse una violazione di dati personali e i sistemi informativi/gli applicativi utilizzati fossero gestiti e messi a disposizione della Provincia, da parte di un Responsabile del trattamento, comunicare l'evento allo stesso Responsabile esterno (Trentino Digitale S.p.a. o altro Responsabile esterno), immediatamente e, comunque, non oltre 24 ore dalla conoscenza, appurando, in collaborazione con il medesimo Responsabile esterno, la sussistenza delle condizioni che determinerebbero l'obbligo di notificazione al Garante e di comunicazione agli interessati;
- in caso in violazione di dati personali, provvedere, in ogni caso, a documentare l'evento e a trasmettere copia della relativa documentazione all'Ufficio Organizzazione e gestione della privacy;

- nel caso di esercizio dei diritti, fornire riscontro all'interessato nei termini di legge, o al Direttore generale (relativamente all'ipotesi di accesso ai dati personali che concerna la Provincia globalmente intesa) secondo le modalità definite al paragrafo 4.2.8 della presente deliberazione;
- mantenere aggiornato (in bacheca, o sul proprio specifico sito *web*) l'elenco dei Responsabili esterni del trattamento della Struttura di competenza, nonché rendere noto (esclusivamente ai dipendenti interessati) l'elenco degli eventuali Amministratori di sistema, nominati dalla Struttura stessa, la cui l'attività riguardasse, anche indirettamente, servizi o sistemi che trattano, o che permettono il trattamento, di informazioni di carattere personale dei dipendenti stessi;
- fornire massima collaborazione al DPO nelle relative attività di consulenza ed *auditing*, agevolandone l'operato e coinvolgerlo nelle questioni concernenti il trattamento dei dati personali prima di iniziare i trattamenti e, in ogni caso, entro termini ragionevoli, nonché documentare le ragioni che hanno portato a discostarsi dai pareri del DPO ;
- rispettare l'obbligo di formazione;
- provvedere affinché copia di ogni eventuale convenzione, sottoscritta con altre P.A. ai sensi degli artt. 50 e ss. del D. Lgs. n. 82/2005, venga trasmessa all'Ufficio Organizzazione e gestione della privacy.

B) Verifica della adeguatezza delle abilitazioni di accesso

Il Preposto è tenuto a:

- individuare i soggetti abilitati ad accedere alle risorse di rete, in relazione ai compiti svolti dal personale che agisce sotto la sua autorità;
- verificare – d'intesa con l'Amministratore di sistema – che la configurazione e l'utilizzo delle risorse, presenti sul *server* di rete della Struttura di appartenenza (unità logiche, cartelle, ecc.), siano conformi a quanto stabilito nella Sezione II (*Misure di sicurezza tecnico-informatiche*) al fine di garantire la riservatezza e l'accesso selezionato alle banche dati contenenti dati personali; la verifica può essere effettuata sulla base delle informazioni che deve comunicare l'Amministratore di sistema sulla composizione dei gruppi di utenti e sulle restrizioni di accesso assegnate alle cartelle di lavoro sui *file system*.

C) Autorizzazione degli Addetti al trattamento

Il Preposto autorizza al trattamento dei dati personali gli Addetti, fornendo loro le istruzioni necessarie ad un corretto trattamento e vigilando sul rispetto delle stesse (artt. 29 e 32 del Regolamento UE 2016/679).
L'atto di autorizzazione, quindi, è integrato con le istruzioni, predisposte in modo coerente con i compiti da svolgere, così come da modello inserito nella Sezione III.
L'autorizzazione deve prescrivere, in particolare, che l'Addetto abbia accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati. Lo stesso atto prevede, inoltre, l'obbligo di archiviare, non appena concluso il trattamento, i documenti e i supporti sui quali sono registrati i dati personali.

L'autorizzazione deve essere predisposta tramite il Registro dei trattamenti (o compilando il modello contenuto nella Sezione III), redatta in duplice originale (uno dei quali viene restituito, dall'Addetto, al Preposto che lo autorizza al trattamento dei dati personali), e sottoscritta per presa visione dallo stesso Addetto. Tale atto dovrà essere aggiornato ogni qual volta si verifichino mutamenti organizzativi che comportino la modifica dei relativi trattamenti e, comunque, con cadenza almeno annuale. L'Addetto, che nell'esercizio dei compiti assegnati tratta dati personali è, quindi, obbligato a sottoscrivere l'atto di autorizzazione del trattamento.

C.1) Autorizzazione al trattamento di dati personali contenuti in archivi e sistemi gestiti contemporaneamente da più Strutture

Nel caso in cui l'Addetto abbia accesso ad archivi o sistemi gestiti in comune da più Strutture (ad es. ambienti applicativi di dominio – quali *SAP* o *PiTre* – o ambienti di produttività individuale), è necessario che lo stesso sia dotato delle prescritte autorizzazioni, che vengono concesse secondo le procedure stabilite. Il Preposto, che è responsabile della corretta attribuzione delle abilitazioni messe a disposizione della Struttura e del personale ad essa assegnato, è tenuto a disciplinare, nell'ambito dell'atto di autorizzazione al trattamento, i limiti di accesso ai dati, le modalità di trattamento degli stessi e quant'altro risultasse necessario per garantire il rispetto della riservatezza e del principio di non eccedenza.

D) Ulteriori misure per il trattamento di particolari categorie di dati e di dati relativi a condanne penali e reati

Con riferimento al trattamento di particolari categorie di dati (art. 9 del Regolamento UE 2016/679 e art. 2-*sexies* D. Lgs. n. 196/2003) e di dati relativi a condanne penali e reati (art. 10 del Regolamento UE 2016/679 e art. 2-*octies*, comma 5, del D. Lgs. n. 196/2003), il Preposto deve verificare:

- che le relative disposizioni di legge, o di regolamento, individuino i tipi di dati che possono essere trattati, le operazioni eseguibili ed il motivo di interesse pubblico rilevante, e
- che le medesime disposizioni normative assicurino che il trattamento sia proporzionato alla finalità perseguita, che sia salvaguardata l'essenza del diritto alla protezione dei dati e che siano previste misure di sicurezza, appropriate e specifiche, per tutelare i diritti fondamentali e gli interessi dell'interessato.

Con riferimento al trattamento di dati biometrici, genetici e relativi alla salute (art. 2-*septies* D. Lgs. n. 196/2003), ulteriormente a quanto sopra previsto, il Preposto deve altresì verificare che i dati stessi siano trattati in conformità alle misure di garanzia disposte dal Garante.

Pertanto, in attuazione di tali compiti, il Preposto deve segnalare, costantemente e tempestivamente, all'Ufficio Organizzazione e gestione della privacy, i trattamenti da inserire nel Regolamento per il trattamento dei dati sensibili e giudiziari, nonché quelli che devono essere modificati o eliminati.

E) Ulteriori misure di sicurezza

Il Preposto al trattamento è tenuto a:

- proteggere i dati personali fin dalla progettazione del trattamento e garantire che siano trattati, per impostazione predefinita, solo i dati necessari al perseguimento delle finalità del trattamento (art. 25 del Regolamento UE 2016/679);
- rispettare le direttive e le misure generali, impartite dalla Giunta provinciale, in materia di trattamento dei dati personali e di sicurezza, nonché curare gli adempimenti da essa stabiliti;
- ottemperare alle istruzioni operative integrative, individuate dalla Struttura competente in materia di sicurezza informatica, in virtù di quanto disposto dalla presente deliberazione, adottando, nell'ambito della Struttura di competenza, le eventuali misure organizzative richieste;
- segnalare, alle Strutture provinciali competenti, la necessità di acquisizione, o di adeguamento, delle dotazioni della Struttura, ovvero la necessità di potenziare i servizi di portineria, onde garantire il rispetto delle disposizioni in materia di sicurezza dei dati personali, concorrendo alla definizione delle priorità nell'ambito della programmazione degli interventi;
- se necessario, adottare, in aggiunta alle misure di sicurezza stabilite dalla Giunta provinciale e previa intesa con la Struttura competente in materia di sicurezza informatica, ulteriori misure di sicurezza, sulla base delle specifiche peculiarità dei trattamenti di competenza della Struttura di appartenenza, idonee ad evitare rischi di distruzione o perdita dei dati, anche accidentale, di accesso non autorizzato, di trattamento non consentito, o non conforme alle finalità della raccolta;
- rispettare le misure di sicurezza previste per gli archivi informatizzati/cartacei contenenti dati personali;

- vigilare, per conto del Titolare, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento dei dati personali, delle istruzioni impartite dal Titolare stesso, nonché sul rispetto delle proprie istruzioni.

F) Amministratori di sistema

Relativamente alla particolare figura dell'Amministratore di sistema, il Preposto deve:

- nominare (se del caso), con riferimento alle risorse dei sistemi operativi ed agli applicativi non gestiti da Trentino Digitale S.p.a., gli Amministratori di sistema, valutandone esperienza, capacità, affidabilità;
- indicare, puntualmente, nell'atto di nomina, l'ambito di operatività dell'Amministratore di sistema;
- verificare, con cadenza annuale, l'operato degli Amministratori di sistema;
- inserire i nominativi degli Amministratori di sistema, le funzioni attribuite e l'ambito di operatività nell'apposita sezione del Registro dei trattamenti;
- conservare, per un periodo minimo di sei mesi, gli accessi logici effettuati dagli Amministratori di sistema;
- rispettare, in generale, le prescrizioni contenute nella deliberazione della Giunta provinciale n. 2081/2016;
- qualora l'attività degli Amministratori di sistema riguardasse, anche indirettamente, servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, rendere nota, o conoscibile, l'identità di tali specifici Amministratori di sistema mediante circolari interne, o forme di comunicazione circoscritte agli interessati.

5.1.3 Persone autorizzate al trattamento – Addetti al trattamento

Il Garante per la protezione dei dati personali ha specificato che "*pur non prevedendo espressamente la figura dell'"incaricato" del trattamento…., il regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento)*".
L'Autorità di controllo ha, poi, ulteriormente precisato che "*Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento possano mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante*".
Conseguentemente, la figura dell'"Incaricato del trattamento", espressamente prevista nella previgente versione del Codice, rientra a pieno titolo nel concetto di persona autorizzata al trattamento ed identifica i collaboratori del Dirigente, assegnati alla Struttura da quest'ultimo diretta (e, quindi, operanti sotto la sua autorità), che effettuano materialmente il trattamento.
Tali collaboratori sono ora qualificati come Addetti al trattamento.
Il personale assegnato ad ogni Struttura provinciale deve essere espressamente autorizzato al trattamento, con atto formale del Preposto (che dovrà utilizzare il modello previsto nella Sezione III della presente deliberazione ed inserito nel Registro dei trattamenti), nonché istruito in tema di protezione dei dati personali; il nominativo dell'Addetto è inserito nel precitato Registro.

E' sempre possibile autorizzare al trattamento un soggetto esterno alla Provincia nei casi – prospettati al paragrafo 5.1.1 – riguardanti collaborazioni per l'espletamento dei compiti

istituzionali (concessioni, appalti, convenzioni, consulenze, collaborazioni, tirocini, ecc.). Va ribadito che possono essere nominati Addetti solo coloro che operano sotto la diretta autorità del Titolare o del Responsabile esterno (in tal caso, la nomina spetta a quest'ultimo), attenendosi alle istruzioni impartite da questi ultimi, i quali, a loro volta, devono vigilare sull'operato degli Addetti.

L'Addetto svolge, nell'ambito del trattamento, meri compiti esecutivi, sulla base delle istruzioni operative ricevute.

La conoscenza dei dati personali, da parte di chi sia stato nominato Addetto al trattamento, non è considerata comunicazione.

Adempimenti dell'Addetto al trattamento

L'Addetto provvede agli adempimenti indicati, a titolo non esaustivo, nell'atto di autorizzazione al trattamento.
Costituisce obbligo di ogni Addetto visionare periodicamente, nell'apposito Registro, i trattamenti allo stesso assegnati, nonché, nel sito istituzionale della Provincia, le deliberazioni della Giunta provinciale in tema di protezione dei dati personali e le circolari emanate nella suddetta materia.

Cautele da adottare, da parte dell'Addetto al trattamento, nell'acquisizione e nel rilascio di documenti contenenti dati personali

Documenti in input

Per "documenti in *input*", si intendono i documenti, o i supporti, contenenti dati personali, acquisiti dalla Struttura ai fini di un loro impiego nel trattamento.
Relativamente al trattamento dei documenti in *input*, è necessario che l'Addetto, tra l'altro, verifichi:

- la provenienza dei documenti;
- che tali documenti siano effettivamente necessari per le finalità del trattamento in corso;
- la tipologia dei dati contenuti, al fine di individuare le modalità, legittime ed idonee, per il trattamento e le misure di sicurezza da attuare;
- che siano garantiti la pertinenza, adeguatezza e limitatezza dei dati personali, rispetto alle finalità del trattamento, nonché l'esattezza e l'aggiornamento dei dati;
- che siano applicate, per la conservazione dei documenti acquisiti, le misure indicate, nella Sezione II, nonché quelle ulteriormente indicate.

L'utilizzo di atti e documenti deve essere limitato al tempo strettamente necessario per eseguire le operazioni di trattamento; al termine dell'attività, la documentazione deve essere riposta nel rispettivo archivio.
L'Addetto al trattamento deve trattare qualunque prodotto dell'elaborazione di dati personali, ancorché non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, stampe, elaborazioni temporanee, ecc.), con le stesse cautele che sarebbero riservate alla versione definitiva.
L'Addetto al trattamento deve informare il Preposto in merito alla necessità di procedere alla cancellazione dei dati personali.

Documenti in output

Per "documenti in *output*", si intendono i documenti, o i supporti, contenenti dati personali prodotti e rilasciati dalla Struttura.
L'Addetto al trattamento deve trattare qualunque prodotto dell'elaborazione di dati personali, ancorché non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, stampe, elaborazioni temporanee, ecc.), con le stesse cautele che sarebbero riservate alla versione definitiva.
L'Addetto al trattamento deve informare il Preposto in merito alla necessità di procedere alla cancellazione dei dati personali.

Nell'ipotesi di documenti in *output*, è necessario, all'atto della consegna o dell'invio, verificare che il destinatario sia legittimato al ritiro e all'utilizzo.
Nel caso in cui fosse formulata, alla Struttura, una richiesta di documentazione, l'Addetto dovrà collaborare, con il Preposto, nell'inquadramento dell'istanza tra i vari possibili diritti di accesso, distinguendo, *in primis*, tra il diritto d'accesso *ex* art. 15 del Regolamento UE 2016/679 e quelli di cui alla L. n. 241/1990, D. Lgs. n. 33/2013 e D. Lgs. n. 195/2005, ovvero, quelli ulteriormente previsti da specifiche disposizioni normative. Qualora la richiesta configuri un accesso ai documenti amministrativi, ovvero un accesso civico generalizzato, o ancora un accesso alle informazioni ambientali, l'Addetto è tenuto ad accertare – se del caso consultando in prima battuta la Struttura competente in materia di diritto d'accesso – i presupposti per corrispondere alla richiesta stessa, mediante l'esibizione/consegna dell'informazione, notizia o documento richiesto. Sarà la Struttura competente in materia di diritto d'accesso, eventualmente, a confrontarsi con l'Umse in materia di protezione dei dati personali per le eventuali limitazioni derivanti dalla normativa di settore.

5.2 Sistema organizzativo provinciale per la protezione dei dati personali

Per "Sistema organizzativo per la protezione dei dati personali" si intende il processo organizzativo determinato dall'insieme di modalità, attività e relazioni che attengono al trattamento e alla protezione dei dati personali e che coinvolge la Provincia autonoma di Trento, sia nei rapporti interni che nei rapporti che intercorrono con il sistema degli Enti, nonché con gli altri soggetti della P.A. (per le funzioni delegate dalla stessa Provincia).
I soggetti principalmente coinvolti nei processi organizzativi descritti, oltre al Titolare, ai Responsabili esterni, ai Preposti e agli Addetti (al trattamento) sono: il Direttore generale, l'Umse in materia di protezione dei dati personali – con il relativo Ufficio Organizzazione e gestione della privacy – la Struttura competente in materia di sicurezza informatica, i Referenti privacy e gli Amministratori di sistema.

5.2.1 Direttore generale

Come già chiarito, il Direttore generale rappresenta una figura fondamentale nel caso di esercizio del diritto di accesso ai dati personali di titolarità della Provincia, globalmente considerata, poiché è tenuto a dare riscontro agli interessati.

5.2.2 Struttura competente in tema di protezione dei dati personali

Per Struttura competente in materia di protezione dei dati personali, si intende l'insieme di funzioni, facenti capo all'Umse per la protezione dei dati personali, caratterizzata dalla demarcazione di seguito descritta.

A) Responsabile per la protezione dei dati personali

Ai sensi dell'art. 37 del Regolamento UE 2016/679, dal 25 maggio 2018 ogni soggetto pubblico è tenuto a nominare un Responsabile della protezione dei dati personali (altrimenti qualificato, in lingua inglese, DPO), che può essere contattato, dagli interessati, per le questioni relative al trattamento dei loro dati personali. Il modello di "richiesta di intervento" è pubblicato sul sito *internet* istituzionale, sia nella sezione relativa alla "Privacy", che nella sezione "Amministrazione trasparente".
La Provincia autonoma di Trento, in coerenza con la necessità di assicurarne la concreta indipendenza, con deliberazione della Giunta provinciale n. 1503 del 15 settembre 2017 ha individuato il DPO in una figura dirigenziale (da ritenere quale livello minimale), condizionandone l'effettivo esercizio delle funzioni alla copertura dell'Ufficio Organizzazione e gestione della privacy. A decorrere dal 10 aprile 2018, pertanto, il ruolo di Responsabile della protezione dei dati

personali è stato assunto dal Dirigente dell'Unità di missione semplice per la protezione dei dati personali.
Allo specifico scopo di garantire la separazione delle rispettive funzioni, il Dirigente dell'Umse per la protezione dei dati personali, nella qualità di DPO, può effettuare un'attività di mera consulenza, non potendo all'opposto interferire nei confronti del Direttore dell'Ufficio Organizzazione e gestione della privacy qualora i suoi compiti si traducano nell'adozione di atti, effettuata per conto del Titolare del trattamento; nell'ambito di tale specifico compito, il Direttore d'Ufficio Organizzazione e gestione della privacy fa direttamente capo al Dirigente generale presso cui è incardinata tale Umse. D'altro canto, dovendo svolgere il DPO funzioni di consulenza nei confronti del Titolare, ed il Direttore dell'Ufficio Organizzazione e gestione della privacy il compito di coordinare le Strutture facenti capo al Titolare, nonché assicurare la cooperazione tra le stesse ed il Responsabile della protezione dei dati, ne consegue un'inscindibile sinergia, organizzativa e funzionale, tra queste due figure. Tale diretta collaborazione (ovvero l'appartenenza alla medesima Struttura in assenza di ulteriori interlocutori) rappresenta una specifica ed evoluta misura organizzativa, adottata dal Titolare, per garantire l'efficace ed efficiente attuazione di un sistema di gestione privacy, altrimenti irrealizzabile, nonché l'indipendenza del DPO e l'effettività delle sue funzioni.
L'innovativa figura prevista dal Regolamento (DPO) svolge funzioni di consulenza e di controllo, nei confronti del Titolare, sugli obblighi derivanti dal Regolamento stesso.
Sulla base della deliberazione della Giunta provinciale n. 1503/2017 il Responsabile per la protezione dei dati: "*informa e fornisce consulenza al titolare del trattamento o al responsabile del trattamento, e ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento 2016/679, nonché da altre disposizioni dell'ordinamento europeo o nazionale relative alla protezione dei dati; vigila sull'osservanza del Regolamento 2016/679, delle altre disposizioni dell'ordinamento europeo o nazionale relative alla protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fornisce, su richiesta del titolare, un parere in merito alla valutazione d'impatto sulla protezione dei dati, vigilandone la relativa applicazione; coopera con l'Autorità garante per la protezione dei dati personali e rappresenta il punto di riferimento, per la medesima Autorità, per questioni connesse al trattamento; presta assistenza, agli interessati, per tutte le questioni relative ai loro trattamenti e all'esercizio dei correlativi diritti*".
E' del tutto evidente come il Responsabile della protezione dei dati personali non sia tenuto e non possa svolgere compiti e/o funzioni di "amministrazione attiva", che competono, in via esclusiva al Titolare del trattamento, onde non incorrere in ipotesi di conflitti di interesse.

Si rammenta, inoltre, come le Linee guida del Comitato europeo per la protezione dei dati (WP 243 rev01) specifichino che "*il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il WP raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD*".

Ai sensi dell'art. 38 del Regolamento UE 2016/679, il Titolare ed il Responsabile del trattamento sono tenuti a coinvolgere il DPO "*tempestivamente e adeguatamente*"; ciò comporta che un incongruo lasso di tempo, un'inadeguata trasmissione di elementi da valutare, e/o eventuali richieste di consulenza che non contemplino o non prospettino, preventivamente, tutti gli aspetti multidisciplinari che caratterizzano le problematiche concernenti la protezione dei dati personali, non potranno essere evase.

Considerata la complessità dell'articolazione provinciale, alla luce degli artt. 37, 38 e 39 del Regolamento UE 2016/679 e dei più recenti orientamenti dottrinali e giurisprudenziali (vedasi T.A.R. del F.V.G. sent. n. 287/2018), delle specifiche Linee guida del Comitato europeo per la

protezione dei dati (WP 243 rev01) e delle ulteriori raccomandazioni dell'Autorità garante (FAQ sul Responsabile della protezione dati in ambito pubblico), altresì valutata la norma UNI 11697:2017, si ritiene che tra i requisiti imprescindibili del DPO dovrebbero essere richiesti: un profilo professionale eminentemente di natura giuridica, con particolari conoscenze in ambito amministrativo, nonché una comprovata esperienza, di durata almeno quadriennale (di cui tre di natura manageriale), specificamente dedicata alla materia della protezione dei dati. Eventuali corsi di specializzazione, oltre che certificazioni/attestati, inoltre, dovranno essere debitamente valutati da parte del Titolare.

B) Ufficio Organizzazione e gestione della privacy:

In virtù della citata deliberazione n. 1503/2017, l'Ufficio Organizzazione e gestione della privacy:

• *cura la predisposizione degli atti normativi e amministrativi, di carattere generale, riguardanti la tutela dei dati personali connessi all'attuazione del Regolamento UE 2016/679;*
• *coordina le strutture provinciali nell'organizzazione del sistema di gestione privacy (valutazione dei rischi, valutazione d'impatto dei trattamenti, attività di formazione ecc.);*
• *cura la redazione del Regolamento per il trattamento dei dati sensibili e giudiziari in collaborazione con le strutture provinciali;*
• *coordina la redazione dell'elenco informatizzato dei trattamenti provinciali e provvede alla conservazione degli elenchi (e/o dei registri) previsti dalla normativa di settore;*
• *garantisce il coordinamento e la cooperazione tra le strutture provinciali ed il Responsabile della protezione dei dati.*

Nell'esercizio delle competenze di cui ai punti precedenti, l'Ufficio Organizzazione e gestione della privacy si avvale della collaborazione dei Referenti privacy.
Tra gli imprescindibili e determinanti compiti dell'Ufficio organizzazione e gestione privacy rientra, inoltre, quello di programmare e coordinare l'attività di formazione nel settore della protezione dei dati personali.

5.2.3 Struttura competente in materia di sicurezza informatica

Spetta alla suddetta Struttura:

- provvedere all'aggiornamento della Sezione II (*Misure di sicurezza tecnico-informatiche*) della presente deliberazione, fornendo le istruzioni operative ad integrazione, specificazione ad eventuale ulteriore chiarimento in tema di misure di sicurezza tecnico-informatiche;
- coordinare i Preposti nell'attuazione dei relativi adempimenti;
- svolgere i controlli e le funzioni specificati nei capitoli della Sezione II, avvalendosi, ove ritenuto opportuno, di soggetti esterni, vigilare sul rispetto delle misure di sicurezza tecnico-informatiche, segnalando eventuali problemi rilevati, in prima istanza, ai Preposti e, in ultima istanza, al Titolare;
- prescrivere, attraverso processi strutturati di *auditing*, le opportune misure tecniche di correzione e adeguamento dei sistemi che risultano disallineati alle misure stesse.

5.2.4 Referente privacy

Il Referente privacy è nominato, presso ciascuna Struttura provinciale (intendendosi per tale ogni Dipartimento, Servizio, Progetto speciale, Incarico dirigenziale, Agenzia e Unità di missione, ecc.), dal responsabile della stessa, allo scopo di operare in raccordo con l'Ufficio Organizzazione e gestione della privacy.
A discrezione dei rispettivi responsabili, possono essere nominati più Referenti privacy per ogni Struttura o, in alternativa, *pool* di Referenti privacy. Il Referente privacy deve rivestire, come

minino, la qualifica di funzionario ed essere adeguatamente competente anche in problematiche giuridico-amministrative.

Il Referente privacy è tenuto a collaborare con il responsabile della Struttura di appartenenza allo scopo di applicare correttamente la normativa in tema di protezione dei dati personali. In particolare, svolge le seguenti funzioni (declinate in modo non esaustivo):

- assicura, ai fini del corretto adempimento della normativa, l'assistenza interna alla/e Struttura/e di appartenenza mediante, in particolare, l'esame delle specifiche problematiche, ivi comprese: (a) l'analisi dell'eventuale *data breach,* la conseguente valutazione in merito alla necessità di notifica/comunicazione e successiva redazione dei relativi moduli; (b) l'eventuale consultazione preventiva del Garante (a seguito della valutazione d'impatto) *ex* art. 36 del Regolamento UE 2016/679; (c) la predisposizione del progetto di norma (in tema di protezione dati) e la successiva trasmissione, al Garante, *ex* art. 36.4 del Regolamento UE 2016/679, tramite il Dipartimento Affari Istituzionali e Legislativi;
- collabora con il Dirigente, istruendo le richieste di parere all'Ufficio Organizzazione e gestione della privacy e/o al Responsabile della protezione dei dati, a seconda dei casi;
- supporta il Dirigente nella redazione ed aggiornamento del Registro dei trattamenti e nell'attuazione delle procedure contenute nel medesimo (ivi compresa la valutazione di impatto), nonché nella segnalazione, all'Ufficio Organizzazione e gestione della privacy, degli aggiornamenti, ritenuti necessari, per il Regolamento dei dati sensibili e giudiziari;
- collabora con il Dirigente nell'adattamento della modulistica, secondo le specifiche esigenze della Struttura di riferimento e nello svolgimento delle procedure finalizzate all'esercizio dei diritti dell'interessato;
- verifica il rispetto degli adempimenti normativi e monitora lo stato di attuazione delle misure di sicurezza in collaborazione con il responsabile della Struttura di appartenenza, con la Struttura competente in materia di sicurezza informatica, nonché con i Referenti informatici;
- provvede all'invio, all'Ufficio Organizzazione e gestione della privacy, della documentazione relativa ai *data breach*, nonché delle convenzioni stipulate con altre P.A. ai sensi del D. Lgs. n. 82/2005;
- provvede alla pubblicazione, nelle modalità *infra* descritte, dell'elenco dei Responsabili esterni della Struttura.

5.2.5 Amministratore di sistema

Relativamente a tale specifica figura, fondamentale anche sotto il profilo del rispetto delle idonee misure di sicurezza e, pertanto, pienamente confermata (per quanto non espressamente prevista dalla più recente normativa in materia di protezione dei dati), nonché con riferimento ad ogni connesso adempimento, si rinvia integralmente alla deliberazione della Giunta provinciale n. 2081/2016.
Nel rispetto di quanto previsto dal Provvedimento del Garante di data 27/11/2008, "*qualora l'attività degli Amministratori di sistema riguardi, anche indirettamente, servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati, nella qualità di datori di lavoro, sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti*". Per tali ragioni, Trentino Digitale S.p.a. è tenuta a comunicare il relativo elenco aggiornato, al Servizio per il Personale, il quale provvederà a renderlo conoscibile (esclusivamente) ai dipendenti provinciali.

5.3 Interessato

Per “interessato” deve intendersi la persona fisica (identificata o identificabile) cui si riferiscono i dati personali.
Per quanto agisca in nome e per conto dell’ente (sia esso un’amministrazione pubblica, una società, un’associazione, ecc.) è qualificabile come “*interessato*” anche il rappresentante legale (Presidente, Sindaco, A.D., ecc.) dell’ente stesso.

SEZIONE II
MISURE DI SICUREZZA
TECNICO-INFORMATICHE

6. MISURE DI SICUREZZA RELATIVE AI SERVER

E' importante precisare, quale premessa alle indicazioni tecniche seguono, che l'orientamento e la scelta principale per l'allocazione dei servizi applicativi è nell'orizzonte dei servizi cloud sia intesi come Cloud Pubblico che come servizi applicativi erogati dal data center della società di sistema Trentino Digitale S.p.a..

Tale orientamento trova fondamento e ***vincolo*** nelle esplicite direttive espresse dal Piano Triennale per l'informatica nella Pubblica Amministrazione oltre che in una visione tecnologica che le Strutture competenti della Provincia stanno perseguendo per la trasformazione digitale progressiva di tutto l'ente.

Nei confronti dei dati personali che vengono memorizzati sui server presenti nella rete locale Provincia, per cui la legge richiede la tutela con misure minime e idonee, deve essere rivolta massima attenzione applicando le regole che seguono.

Le misure si applicano, oltre alla gestione di file system locali, anche quindi a sistemi cloud storage pubblico o ibrido come ad esempio Google Drive, Owncloud, Dropbox o altri servizi che il mercato mette a disposizione.

6.1 Misure di sicurezza organizzative

Il **Preposto** - d'intesa con l'Amministratore di sistema - **verifica** che la configurazione e l'utilizzo delle risorse presenti sul server di rete della propria struttura (unità logiche, cartelle) sia funzionale alle **esigenze di riservatezza** delle banche dati contenenti dati personali.
In particolare, verifica che la configurazione e l'utilizzo delle risorse di rete sia conforme all'impostazione di cui al Capitolo 8 *Misure di sicurezza relative alle risorse di rete e dei PC*, disponendo, in particolare, l'accesso differenziato, in base ad abilitazioni personali o per gruppi di lavoro e in relazione ai compiti svolti dal personale.

6.2 Misure di sicurezza logistiche

Per i server fisicamente presenti nelle location amministrate da Dipartimenti o Servizi della Provincia, devono essere adottate le misure logistiche illustrate nei seguenti paragrafi, idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso fisico non autorizzato;
- distruzione o perdita dei dati dovuta ad eventi fisici.

L'Amministratore di sistema e i tecnici che hanno accesso ai locali del server devono informare il Preposto nel caso in cui riscontrino il mancato rispetto delle misure di sicurezza logistiche di seguito elencate (ad esempio locali server lasciati aperti o mancata custodia delle chiavi degli stessi).

Si ribadisce che è sempre auspicata la centralizzazione e virtualizzazione dei server presso il data center di Trentino Digitale S.p.a., considerando residuali

situazioni in cui vi sono requisiti funzionali che costringono progetti di gestione all'interno del perimetro LAN PAT.

6.2.1 Protezione del server da accesso fisico non autorizzato

Per tutelare la riservatezza dei dati personali accessibili sul server e per proteggere l'efficienza delle apparecchiature, l'accesso ai locali in cui vi sono uno o più sistemi server è limitato nel seguente modo:

- le apparecchiature server devono essere poste in apposite stanze, destinate a contenere soltanto il server stesso ed eventualmente le apparecchiature di rete;
- dove sia logisticamente difficoltosa l'ubicazione del server in un apposito locale e per le strutture esistenti che non rispondono ai requisiti di cui al punto precedente, vanno individuate soluzioni organizzative alternative (es. armadi chiusi e appositamente allestiti) che offrano le medesime garanzie di sicurezza;
- l'accesso ai locali server è protetto tramite la chiusura a chiave del locale;
- la chiave è custodita da personale incaricato della custodia dal Preposto;
- il personale incaricato della custodia delle chiavi è tenuto a riporle in un luogo non agevolmente accessibile ad altri;
- in sede di progettazione e di realizzazione di nuove strutture adibite ad uffici provinciali ovvero in sede di ristrutturazione di edifici esistenti, vanno tenute presenti le esigenze di tutela dei dati personali;
- se il locale è situato in una posizione tale da rendere agevole un'intrusione dall'esterno è opportuno munirlo della protezione adeguata, quale ad esempio l'apposizione di barre anti intrusione alle finestre.

In sede di progettazione di nuovi uffici, va tenuto presente che utilizzando, per la chiusura della stanza, dispositivi tecnici quali chiavi di tipo *badge* o chiavi di accesso in grado di consentire il rilevamento degli ingressi, è possibile assolvere, in via contemporanea, all'adempimento del controllo dell'accesso fisico al server ed al locale ed a quello relativo alla compilazione del registro degli accessi, che, in tal caso, non sarebbe richiesta.

Accesso di personale interno della struttura

Possono accedere ai locali in cui sono presenti uno o più sistemi server solo:

- il Preposto;
- l'Amministratore del sistema;
- il custode delle chiavi;
- il personale della struttura che deve accedervi per l'espletamento dei compiti propri, per le necessità di gestione e manutenzione dei sistemi (ad es. il personale Preposto al cambio giornaliero delle cassette di backup), dei locali e degli impianti, nonché per attività di pulizia ed affini ed altre attività comunque indispensabili.

Accesso di personale esterno alla struttura

Gli interventi di manutenzione o adeguamento sui server, sui locali che li contengono e sui relativi impianti, sono richiesti, o comunque autorizzati, dal Preposto Quando, per l'espletamento di compiti di servizio e per altre attività, è necessario consentire l'accesso a personale esterno o a personale dipendente della Provincia non appartenente alla Struttura, vanno osservate le seguenti misure:

- il locale viene aperto dal personale custode delle chiavi;

- ciascun intervento è annotato su un apposito registro, conservato nella stanza del server recante data e orario dell'intervento (inizio-fine), tipo di intervento, nome, cognome del tecnico intervenuto/ditta o struttura, firma;
- al termine dell'intervento, l'incaricato della custodia della chiave provvede alla chiusura dei locali;
- nessun soggetto estraneo può accedere ai sistemi server se non accompagnato dal personale indicato nel paragrafo "Accesso di personale interno della struttura".

Accesso di personale esterno alla struttura per servizi di pulizie o simili

- Non sussiste la necessità di effettuare, quotidianamente, le operazioni di pulizia nella stanza contenente il server: le giornate in cui il personale addetto alle pulizie accede, alla medesima, sono programmate, anche al fine dell'apertura del locale;
- è preferibile che le operazioni di pulizia si svolgano quando è presente il personale addetto alla custodia della chiave, che provvede personalmente all'apertura;
- ove non sia possibile la presenza del personale addetto alla custodia della chiave, in quanto l'intervento di pulizia si svolge al di fuori dell'orario di servizio per altre cause ostative, in via eccezionale il locale rimane aperto al fine di consentire l'ingresso del personale addetto, limitatamente ai periodi in cui è stato programmato l'intervento di pulizia;
- gli accessi sono annotati nell'apposito registro di cui sopra.

6.2.2 Protezione dei dati dal rischio di perdita dovuta ad eventi fisici

Tra gli eventi fisici, che possono portare alla perdita dei dati per distruzione delle apparecchiature, vengono considerati incendio, surriscaldamento delle apparecchiature, anomalie dell'alimentazione elettrica e altri eventi (allagamenti, crolli ecc.).

Contromisure per il rischio di incendio

Contro l'eventualità che un incendio nei locali in cui sono custoditi i sistemi server possa causare danni irreversibili ai dati, sono necessarie le seguenti misure di sicurezza:

- in prossimità del server deve essere installato un dispositivo antincendio. In sede di progettazione e di realizzazione di nuove strutture adibite ad uffici provinciali ovvero in sede di ristrutturazione di edifici esistenti, vanno tenute presenti le esigenze di sicurezza, ad es. dotando i locali di impianti di spegnimento automatico degli incendi;
- **le cassette di backup devono essere conservate in un armadio ignifugo, chiuso a chiave, dislocato in un locale diverso da quello che ospita il server;**
- **è indispensabile implementare una soluzione di backup centralizzata presso il datacenter Trentino Digitale S.p.a., prima di entrare in produzione e chela stessa sia sottoposta a collaudo.**

Contromisure per le anomalie nell'alimentazione elettrica

Contro l'eventualità che anomalie dell'alimentazione elettrica dei sistemi server possano danneggiare i dati, è necessario predisporre il collegamento ad un gruppo statico di continuità.

Contromisure per altri eventi (allagamenti, crolli ecc.)

In sede di progettazione e di realizzazione di nuove strutture adibite ad uffici provinciali ovvero in sede di ristrutturazione di edifici esistenti, vanno tenute presenti le esigenze di sicurezza evitando, ad esempio che i locali contenenti i server siano ubicati in scantinati o piani seminterrati (a rischio allagamenti).

6.3 Misure di sicurezza tecniche, informatiche e procedurali

La sicurezza dei server deve essere tutelata con le misure tecniche, informatiche e procedurali illustrate nei seguenti paragrafi che siano idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso logico non autorizzato o non conforme alle regole;
- distruzione o perdita dei dati dovuta ad attacchi esterni (es.: virus);
- distruzione o perdita dei dati dovuta ad attacchi di malintenzionati;
- perdita accidentale dei dati.

6.3.1 Protezione da accessi logici non autorizzati

Per **accesso logico**, nel contesto di questo documento, si intende l'accesso ai dati contenuti sul server attraverso l'utilizzo di un computer connesso in rete. Si tratta, cioè, dell'accesso e dell'utilizzo dei dati personali tramite i PC, collegati alla rete, a cui è connesso il server o dell'accesso ai dati dalla console del server stesso. L'accesso logico è permesso a chi digita la corretta combinazione di identificativo utente (user-id) e parola chiave (password).

I sistemi operativi consentono di:
- regolare l'accesso, disponendo di caratteristiche personalizzabili in grado di implementare vari gradi di sicurezza, garantendo contro il rischio di utilizzo dei dati da parte di persone non autorizzate;
- mantenere una traccia di tutti gli accessi (*log*), e quindi conoscere quando e che utente si è connesso al sistema e quali utenti hanno cercato di accedere a risorse non autorizzate;
- per quanto riguarda le misure di sicurezza da adottare e i comportamenti che devono tenere gli utenti, si rinvia alle indicazioni riportate nel capitolo 8 (*Misure di sicurezza relative alle risorse di rete e dei PC*) e al capitolo 9 (*Misure di sicurezza relative alle postazioni di lavoro*).

6.3.2 Protezione dai virus

I virus sono particolari programmi, predisposti per essere eseguiti all'insaputa dell'utente, che possono causare danni ai dati memorizzati sul computer o al sistema operativo del computer stesso. Sui sistemi server, l'Amministratore di sistema installa e provvede a mantenere un software antivirus, con aggiornamento periodico automatico, che garantisce una protezione idonea ad evitare il verificarsi di danni ai dati.

6.3.3 Protezione da malintenzionati

Ogni computer collegato in rete può essere oggetto di tentativi di connessione effettuati da soggetti che utilizzano altri computer collegati alla rete. Quando il computer è collegato a Internet, le intrusioni possono teoricamente essere effettuate da computer connessi a Internet situati in una qualsiasi parte del mondo.

Per fare fronte a questo rischio, le postazioni di lavoro ed i server della struttura sono collegati a Internet attraverso la rete Telpat, per cui la protezione dalla distruzione o perdita dei dati, dovuta ad attacchi di malintenzionati che agiscono collegandosi dall'esterno, via Internet, è garantita dai sistemi *firewall* gestiti da Trentino Digitale S.p.a.
La difesa, dagli attacchi di questo tipo, è comunque assicurata solo se viene data puntuale applicazione a tutto il complesso delle regole di sicurezza comprese nel presente documento.

6.3.4 Protezione dal rischio di perdita accidentale dei dati

Per ovviare al rischio di perdita accidentale dei dati, sui server è presente un sistema di salvataggio automatico degli stessi mediante copia automatica (backup).
Il salvataggio automatico:

- garantisce il recupero dei dati a fronte di guasti hardware o software, limitando i disagi connessi con la discontinuità del servizio;
- consente di recuperare dati o file accidentalmente eliminati o erroneamente modificati.

Sistemi server non gestiti da Trentino Digitale S.p.a.

La politica di backup deve assicurare almeno le medesime garanzie di efficienza e sicurezza fornite dal sistema di cui sopra e comunque il rispetto delle misure minime di sicurezza contenute nella circolare Agid n. 2/2017 di seguito "circolare AGID".

La responsabilità, del rispetto delle misure di sicurezza, grava sul Dirigente della Struttura che utilizza il server non gestito da Trentino Digitale S.p.a..

Politica dei backup

Le risorse in gestione a Trentino Digitale S.p.a. sono connesse con il sistema centralizzato di back-up situato nel datacenter dell'azienda. Per queste, non è necessario nessun intervento locale ed il periodico salvataggio dei dati viene eseguito in maniera completamente automatizzata.
Per i dettagli si rimanda all'Appendice 6 – Politiche di backup del Piano annuale ICT.
Il backup è gestito in automatico dal sistema server durante la notte (tra le 21:30 e le 24:00 di ogni giorno lavorativo); a livello della struttura, nel caso di sistemi non connessi al sistema centralizzato di backup, sono presenti cinque cassette magnetiche (DAT, DLT o AIT), una per ogni giorno della settimana (da lunedì a venerdì), etichettate con il nome del giorno.
Il **referente informatico** della Struttura, o altra persona incaricata dal Preposto, deve eseguire giornalmente le seguenti operazioni:

- controllare, ogni mattina, l'esito del backup giornaliero (l'esito negativo del backup viene comunicato tramite e-mail al referente informatico della struttura): il file di log contiene il rapporto dettagliato di tutte le operazioni che il backup ha effettuato;
- contattare, in caso di esito negativo del backup, l'Amministratore di sistema.

Nel caso di sistemi non connessi al sistema di backup centralizzato, è necessario ottemperare anche agli adempimenti seguenti:

- sostituire, ogni mattina, sul sistema server, la cassetta magnetica contenente i dati di backup del giorno precedente con quella etichettata con il nome del giorno in corso;
- collocare la cassetta contenente i dati di backup del giorno precedente, in un locale diverso da quello in cui è dislocato il sistema server, in armadi ignifughi chiusi a chiave; l'accesso agli armadi è consentito al solo personale autorizzato e deve essere protetto con misure di sicurezza fisiche non inferiori a quelle adottate per il server (in quanto le cassette contengono copia di tutti i dati presenti sul server);
- provvedere alla manutenzione dell'unità nastro. Utilizzare la cassetta di pulizia per mantenere sempre in buona condizione di funzionamento il lettore.

E' consigliabile conservare, per un anno, la cassetta relativa all'ultimo backup di ogni mese; le cassette vanno sostituite dopo circa 50 cicli di utilizzo e/o comunque seguendo le istruzioni del costruttore.

7. MISURE DI SICUREZZA RELATIVE ALLA RETE DI INTERCONNESSIONE (TELPAT)

7.1 Misure logistiche

Per un'adeguata collocazione delle apparecchiature di rete della Provincia, devono essere adottate, in quanto compatibili, le misure logistiche già illustrate nel capitolo 6 relativo ai server. Va ricordato, infatti, che la sicurezza dell'intera rete può essere messa a rischio se un malintenzionato ottiene l'accesso fisico, per un tempo sufficiente, ad una o più apparecchiature di rete.

7.2 Regole per connettersi alla rete Telpat (rivolto agli enti ai quali la Provincia mette a disposizione la rete)

La rete Telpat, negli anni, ha subìto significativi mutamenti, sia relativamente alla infrastruttura tecnologica che alla sua funzione. E' passata, infatti, dallo stato di "Rete chiusa", che ha caratterizzato l'inizio della sua storia allo specifico scopo di condividere informazioni con altri soggetti della Provincia, a quello di rete connessa a Internet, fino alla situazione attuale nella quale, di fatto, è un network, di vaste dimensioni, a cui possono accedere tutti i soggetti della amministrazione pubblica locale della Provincia di Trento, per usufruire di servizi informativi centralizzati.

Il ruolo acquisito ha, necessariamente, innalzato il livello di criticità della disponibilità del servizio di connettività, riducendo drasticamente il controllo che la Provincia può esercitare sui siti periferici interconnessi. Infatti, se risulta evidente che il non corretto funzionamento della rete può causare gravi disservizi (un esempio per tutti la posta elettronica), non è altrettanto chiaro che la Provincia, ovvero il soggetto che mette a disposizione di tutta la pubblica amministrazione locale questo fondamentale servizio, non ha, di fatto, la possibilità di controllare che le reti locali collegate rispettino un set minimo di misure di sicurezza il quale, oltre ad essere in gran parte previsto dalla normativa vigente, determini la riduzione del rischio di compromettere la rete provinciale.

Lo scopo di questo paragrafo è quello di definire gli standard minimi di misure di sicurezza per tutti gli enti, della pubblica amministrazione locale, che si interconnettono con la rete provinciale. Gli standard sono stati elaborati per minimizzare l'esposizione della rete provinciale ai pericoli derivanti da reti, scarsamente protette, che fungono da teste di ponte per virus, intrusioni informatiche, spyware etc..
I pericoli che si intendono evitare sono la perdita di dati, il danneggiamento o malfunzionamento dei sistemi e/o della rete provinciale, etc..

7.2.1 Misure minime di sicurezza per l'utilizzo della rete Telpat

Gli enti, che si interconnettono con Telpat, devono applicare, alla loro struttura informatica, le misure minime di sicurezza specificate nella circolare AGID ed in particolare:

- che gli apparati informatici siano provvisti di una procedura che preveda l'autenticazione univoca dell'operatore;
- che agli operatori siano impartite idonee istruzioni, sull'adozione delle necessarie cautele, per assicurare la riservatezza delle informazioni ed il corretto funzionamento dei sistemi, con l'obiettivo di non causare malfunzionamenti della rete;
- che vengano disattivate le credenziali di autenticazione degli operatori non più in servizio;

- che agli operatori siano impartite istruzioni per non lasciare incustodito e accessibile lo strumento elettronico;
- che venga effettuata una verifica periodica degli operatori abilitati;
- che gli strumenti informatici siano dotati di software antivirus, aggiornati periodicamente.

In aggiunta a quanto previsto dalla succitata circolare AGID, sarà cura dell'ente garantire che la propria rete locale non abbia altre connessioni di rete con l'esterno, ad eccezione del collegamento con Telpat, salvo i casi di cui al successivo paragrafo.

7.2.2 Ulteriori misure

Nel caso in cui, per improrogabili necessità operative, l'ente sia dotato di un ulteriore collegamento geografico (es. connessione ad Internet con un operatore pubblico), ovvero si trovi nella necessità di dover garantire, a terzi, accessi remoti alla propria rete, non verificabili dalla Provincia (ad esempio, per ragioni di assistenza tecnica o di connettività ad Internet), dovrà darne immediata comunicazione alla Struttura, competente in materia di sicurezza di Trentino Digitale S.p.a., affinché venga installato un idoneo apparato hardware (firewall) per garantire la difesa perimetrale

8. MISURE DI SICUREZZA RELATIVE ALLE RISORSE DI RETE E DEI PC

L'operatore, tramite la procedura di accesso logico che prevede l'utilizzo di un identificativo utente (user-id) e di una password, può accedere ad una stazione di lavoro (PC) connessa alla rete della struttura. In questo modo l'operatore può:

- accedere alle risorse presenti fisicamente sulla macchina stessa (dischi fissi);
- accedere alle risorse di rete (cartelle del disco fisso del server su cui l'utente ha diritto di accesso);
- condividere, con altri utenti risorse quali file, cartelle (ad es. dischi U e T) e stampanti;
- condividere con altri utenti applicazioni;
- usufruire della centralizzazione delle operazioni di backup (nel caso in cui i dati siano salvati sul server) e di aggiornamento software.

8.1 Descrizione della configurazione standard delle stazioni di lavoro

Le unità logiche disponibili, in base alle configurazioni standard possono essere in sintesi le seguenti:

A) Unità locali del computer

C:\ D:\ (individuate anche con lettere diverse) = unità logiche/dischi installati fisicamente sul PC, altrimenti detti dischi fissi o locali.
Unità escluse dalla garanzia del salvataggio automatico dei dati (backup notturno) attiva sul server. Da ciò derivano rischi per la sicurezza dei dati e la loro conservazione, se non vi è un accorto utilizzo del computer e un salvataggio coscienzioso dei dati. L'utente deve evitare di conservare i dati di cui va garantita la sicurezza su queste unità. Infatti è sempre possibile che il danneggiamento del computer porti alla perdita dei dati. In secondo luogo, per quanto difficile, non è del tutto impossibile che vi sia un accesso fisico alla macchina, in assenza dell'utente, anche da parte di estranei. Per il malintenzionato che ottiene l'accesso fisico alla macchina, l'accesso ai dati presenti sulla stessa non presenta particolare difficoltà.

B) Unità di rete individuale

Y: = L'unità logica/disco Y è la cartella individuale dell'utente sul server di rete. L'accesso è, cioè, consentito all'utente che si è correttamente autenticato all'atto di accedere al PC locale collegato in rete. Questo disco deve essere usato per memorizzare dati che non necessitano di essere condivisi con altri utenti (quelli per cui altri non hanno l'autorizzazione al trattamento o dati riservati).
Ogni utente può vedere sempre e solo la propria cartella

personale, e non quelle degli altri utenti. Per contro, l'Amministratore di sistema può vedere e modificare le cartelle e i dati di tutti. Gli utenti hanno accesso in lettura e scrittura al proprio disco Y. Per l'unità Y è garantito il salvataggio automatico dei dati (backup notturno).
Tale disco logico ha una capacità standard di base per ogni utente, ampliabile su richiesta motivata.

Nota Bene: se si accede alla rete della Struttura utilizzando il proprio identificativo utente e la propria password, da un **qualsiasi PC** connesso, si avrà accesso al **proprio disco Y**. In altre parole, in caso di malfunzionamento o arresto momentaneo della propria stazione di lavoro, l'utente può servirsi della stazione di lavoro di un collega per accedere ai propri dati conservati sul disco Y (Solo per i pc della stessa Struttura).

C) Unità di rete comuni

T: = unità logica/disco di transito utilizzabile per il passaggio di dati tra utenti. Unità **esclusa** dalla garanzia del salvataggio automatico dei dati (backup notturno). Infatti il disco T non è oggetto di backup giornaliero.
Tutti gli utenti hanno accesso a T:\ in lettura e scrittura, anche sui file di altri utenti.
NB: tale disco deve essere assolutamente **utilizzato solo per il transito**, di dati e programmi, da un utente all'altro; ogni fine settimana, infatti, il disco T:\ viene cancellato per recupero spazio.
I dati, pertanto, vanno spostati su altro disco di rete e cancellati dal disco T:\ dopo il loro utilizzo.
Nel caso di server centralizzati, il disco T:\ è comune per tutti gli utenti della Provincia

U: = unità logica/disco dati degli utenti. Unità garantita dal **salvataggio automatico dei dati** (backup notturno). Questa unità logica/disco, all'inizio accessibile a tutti gli utenti sia in lettura sia in scrittura, **consente una personalizzazione dei diritti di accesso**. La personalizzazione, di norma, va richiesta all'Amministratore di sistema che può creare dei gruppi di utenti secondo le esigenze della Struttura. Può anche essere operata dagli stessi utenti all'atto della creazione di una nuova directory. In questo caso l'utente che ha creato la directory ha anche la possibilità di cambiare le regole di accesso degli altri utenti a quella particolare directory. Ogni directory può possedere delle restrizioni che permettono l'accesso personalizzato solo a determinati utenti, individuati a seconda del gruppo di lavoro cui appartengono o delle specifiche competenze/esigenze del singolo utente. Tali diritti di accesso personalizzato (ad es. sola lettura, lettura e modifica, cancellazione su singoli file o directory), sono connessi all'account dell'utente già esistente e non richiedono pertanto la creazione di nuovi identificativi di utente. L'unità U:\ deve essere utilizzata per i documenti che devono essere condivisi

tra più persone della Struttura e che devono essere salvati sul backup giornaliero.

Il disco pertanto va organizzato, di norma, creando delle directory protette, tenendo conto dei gruppi di lavoro esistenti all'interno dei servizi.

C) Unità di cloud storage pubblico

Si tratta di unità logiche collocate presso un operatore SPC (Service Public Cloud) che mette a disposizione servizi, connessi o meno a suite di produttività individuale o a servizi di messaging, per la gestione di file di rete.

Per questo tipo di servizi sono formalizzate policy specifiche oltre a valere le raccomandazioni e le direttive per i dischi di rete, ove applicabili.

A fronte di particolari esigenze nella configurazione della rete e dei PC, le Unità logiche/dischi potrebbero essere individuate da lettere diverse rispetto a quelle sopra indicate. In questo caso è necessario contattare l'Amministratore di sistema al fine di censire la situazione della propria struttura.

8.2 Misure di sicurezza informatiche

In base alla configurazione appena descritta, vanno adottate le seguenti misure:
per la memorizzazione dei dati deve essere privilegiato l'utilizzo delle risorse di rete (Y e U) o del servizio di cloud storage, evitando l'uso delle unità logiche presenti fisicamente sul PC (dischi fissi/locali C e D); in ogni caso, le elaborazioni riguardanti dati personali vanno memorizzate sui dischi di rete U e Y.
Anche se alcuni programmi applicativi consentono la protezione dei singoli file mediante l'apposizione di specifiche password, tale pratica va evitata.

Cartelle, con accesso per gruppi di lavoro, sull'unità U

Per un ottimale utilizzo delle risorse di rete, sono predisposte, sul disco U, cartelle con accesso limitato per gruppo di lavoro (alcuni in scrittura, altri in lettura).
È così possibile usare cartelle a supporto della divisione del lavoro per gruppi (chi svolge le medesime attività può condividere i dati con i colleghi) senza sacrificare la sicurezza dei dati, in quanto l'accesso è limitato solo a chi, nell'ambito della struttura, è effettivamente Addetto al trattamento dei dati. L'uso del disco U non richiede la creazione di ulteriori user-id e password, in quanto i gruppi di utenti vengono creati sulla base degli utenti già esistenti.

L'organizzazione del disco U, per gruppi di lavoro, richiede un'analisi delle esigenze organizzative della Struttura, per individuare la configurazione adatta e la creazione, da parte dell'Amministratore di sistema, di gruppi di abilitazione, nei quali gli utenti saranno inseriti a seconda delle attività cui sono preposti.

Ciascun utente, con l'user-id e la password di accesso alla rete, è contemporaneamente abilitato all'accesso alle sole cartelle protette del disco U riservate ai gruppi di lavoro a cui appartiene.

Il responsabile della Struttura è tenuto a segnalare la variazione della composizione dei gruppi all'Amministratore di sistema, per l'adeguamento delle abilitazioni; l'Amministratore deve configurare i permessi sul disco U e la composizione dei gruppi di lavoro. L'eventuale presenza, sul disco U, di cartelle denominate secondo la comune identificazione dei gruppi di lavoro (ad esempio "segreteria del Dirigente"), sulle quali non vengono applicate limitazioni coerenti con la denominazione stessa (cioè accesso non limitato al solo gruppo ma indifferenziato per tutti gli utenti della Struttura), ***costituisce una falla nella sicurezza perché può indurre gli utenti a ritenere protetta la memorizzazione nella cartella stessa***.

Per questo motivo, l'Amministratore di sistema e il responsabile della Struttura, supportato dal proprio referente informatico, si devono attivare al fine di verificare la correttezza delle limitazioni di accesso sul disco U. A tal fine, l'Amministratore di sistema deve segnalare periodicamente, al referente informatico e al responsabile della Struttura, quali utenti fanno parte dei gruppi di lavoro che hanno accesso alle cartelle della directory principale dell'unità U.

Per i servizi Cloud è necessario che l'Amministratore di sistema provveda alle corrette configurazioni seguendo le policy dedicate.

Trattamento dei dati di responsabilità di un unico Addetto

Per la memorizzazione dei dati che devono rimanere riservati e visibili al solo utente (Addetto al trattamento), deve essere prioritariamente utilizzato il disco Y, anziché i dischi fissi/locali. Infatti, come è già stato evidenziato, le esigenze di riservatezza e sicurezza sono garantite solo memorizzando i dati sul server.

Uso dei dischi fissi/locali (C:\ e altri)

L'utilizzo dei dischi fissi/locali presenta rischi di integrità sotto il profilo della sicurezza dei dati. Pertanto, se non è possibile usare le unità di rete (Y e U), è responsabilità dell'utente effettuare backup periodici con propri dispositivi personali.

Regole per l'utilizzo di servizi di Cloud Computing

Il paradigma cloud si sta affermando, in modo costante, come modalità di utilizzo e di procurement di servizi applicativi per la PA. Il contesto di riferimento normativo è quello del Piano Triennale per l'Informatica nella PA[1], piano che ricordiamo nasce per il triennio 2017-2020 per poi essere rinnovato di anno in anno, rappresentando sempre quindi l'evoluzione progressiva triennale.
Il Cloud Storage, in particolare, è un'area di conservazione dei dati su computer in Internet dove i dati stessi sono memorizzati su molteplici server virtuali generalmente ospitati presso strutture di terze parti o su server dedicati. I dati salvati sui sistemi di Cloud Storage sono online con gli SLA offerti dagli operatori certificati Agid.
Considerato il fatto che i dati, in tal caso, sono archiviati on line (internet), gli stessi sono facilmente condivisibili con strutture interne ma anche con soggetti esterni alla Provincia. Nello stesso tempo conservare (Storage) nella nuvola (Cloud) vuol dire condividere, online, file e cartelle disponibili ovunque e attraverso qualunque dispositivo (computer, smartphone, tablet etc…).
Molti utenti, nella vita privata, utilizzano cloud storage pubblici. Questo permette accessi ai propri file e dati attraverso vari device. Se impiegati in un contesto lavorativo si introducono rischi che riguardano la sicurezza, la privacy, i diritti d'autore e il tempo di conservazione dei dati (retention) di interesse provinciale.

[1]https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/stabile/

In generale, si chiede di seguire le seguenti indicazioni:

- porre attenzione nella memorizzazione di file che contengono dati personali e sensibili;
- se si stanno condividendo, sul cloud storage, strumenti con altri collaboratori interni o esterni, verificare attentamente i diritti d'accesso sui file condivisi, evitando di concedere permessi non appropriati e revocandoli quando non servono più;
- analogamente a quanto avviene quando si allegano documenti in posta elettronica o si condividono file, su file system di rete, evitare di condividere link (URL) per il download di documenti contenenti dati personali;
- il fornitore di servizi di cloud storage deve rispettare quanto indicato nel Capo V - Trasferimento di dati personali verso paesi terzi e organizzazioni internazionali - del Regolamento UE 2016/679.

9. MISURE DI SICUREZZA RELATIVE ALLE POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso delle apparecchiature che il datore di lavoro (Provincia) mette a disposizione dei dipendenti (utenti).

9.1 Misure di sicurezza logistiche

Un'adeguata protezione dei **luoghi di lavoro** serve a garantire la sicurezza dei dati personali custoditi al loro interno. Per assicurare la sicurezza di dati devono essere adottate misure logistiche idonee a proteggere i documenti, supporti informatici e apparecchiature rispetto al rischio di:
- accesso fisico non autorizzato;
- distruzione o perdita dei dati dovuta ad eventi fisici.

9.1.1 Protezione delle postazioni da accesso fisico non autorizzato

Per accesso fisico s'intende l'accesso ai locali in cui vi sono una o più postazioni di lavoro dotate di PC. Le misure di sicurezza devono eliminare o ridurre il rischio di accesso fisico ai locali o di intrusione da parte di persone non autorizzate. L'accesso fisico alla postazione di lavoro collegata in rete, da parte di estranei non identificati, rappresenta comunque un potenziale rischio per la sicurezza dei dati custoditi sulle postazioni di lavoro, anche se la persona non può conoscere le password. Per evitare questo rischio, si devono adottare le seguenti misure di sicurezza:

9.1.1.1 Personale interno alla Struttura

Le postazioni di lavoro sono accessibili solo da chi ha titolo, in qualità di Preposto o Addetto al trattamento, Amministratore di sistema, nei limiti in cui ciò sia funzionale allo svolgimento dei compiti della Struttura, o per lo svolgimento di attività di manutenzione, di pulizia e affini, nonché per altre attività comunque indispensabili.
L'accesso fisico ai luoghi di lavoro è protetto tramite la presenza di personale di portineria ovvero attraverso la chiusura delle vie di accesso; in ogni caso, gli uffici aperti al pubblico devono essere presidiati da personale di portineria; negli orari diversi da quelle di servizio, ove non sia presente un presidio, la porta di accesso all'edificio deve rimanere chiusa.

9.1.1.2 Personale esterno alla struttura

La persona esterna può accedere ai locali solo quando è presente il dipendete della Struttura; la persona esterna deve farsi riconoscere dal personale di portineria e seguire le regole, stabilite dal Preposto, per l'accesso del pubblico alla Struttura stessa.

9.1.1.3 Interventi di assistenza e manutenzione

9.1.1.3.1 Assistenza in remoto

Gli interventi di assistenza, installazione e aggiornamento dei software e, in generale, quelli volti a fronteggiare guasti o temporanei black-out delle postazioni di lavoro, sono di norma effettuati da Trentino Digitale S.p.a. tramite il servizio di assistenza e amministrazione remota sui PC e sui server di rete, denominato *System Management*, senza la necessità dell'intervento di un tecnico informatico presso la postazione di lavoro. In caso di guasto, o malfunzionamento, del proprio PC, l'utente può attivare l'intervento di assistenza remota, contattando telefonicamente il Customer service Desk di Trentino Digitale S.p.a..

9.1.1.3.2 Assistenza con intervento locale del tecnico

Qualora siano necessari interventi di manutenzione sulla macchina o di assistenza, adeguamento, ecc. sulla postazione di lavoro, è necessario che l'utente o il referente informatico o, in loro assenza, altro dipendente della Struttura, assista alle menzionate operazioni.
La segreteria deve trattenere e conservare copia del rapporto di intervento, rilasciato dalla ditta intervenuta. Il rapporto deve contenere data e orario dell'intervento (inizio e fine), descrizione sintetica del tipo di intervento, nome e cognome del tecnico intervenuto e della ditta, firma del tecnico e dell'utente che assiste all'intervento. Ove non già presenti, tali dati devono essere apposti dal personale di segreteria in presenza del tecnico intervenuto. **La descrizione dell'intervento non può contenere codifiche dal significato non immediatamente comprensibile per l'utente che sottoscrive il rapporto.**

9.1.2 Protezione dei dati dal rischio di distruzione o perdita a causa di eventi fisici

Gli eventi fisici, che possono costituire fonte di rischio, per le postazioni di lavoro, sono quelli indicati nel paragrafo relativo ai server.
Al fine di ridurre al minimo i rischi di distruzione o perdita di dati, è consigliabile:

- prediligere il lavoro sui dischi di rete, la cui protezione è assicurata dalle misure di sicurezza e di salvataggio automatico adottate per i server;
- in caso di utilizzo dei dischi installati fisicamente sul pc (C e D), effettuare periodici backup dei dati, su supporti magnetici, da conservare secondo quanto disposto nell'apposito paragrafo. Si ribadisce che, in quest'ultimo caso, la responsabilità di effettuare i backup periodici è a carico dell'utente.

9.2 Misure di sicurezza tecniche, informatiche e procedurali

9.2.1 Protezione da accessi logici non autorizzati

L'accesso logico alle postazioni di lavoro è consentito attraverso l'utilizzo combinato di una parola chiave (password) e di un identificativo utente (user-id) che autentica l'utente sul server della rete. In assenza dell'autenticazione, la postazione non è immediatamente utilizzabile. A ciascun utente, all'assegnazione della dotazione informatica, viene attribuito un identificativo utente (user-id), univoco ed immutabile, ed una password personale, segreta e sostituibile dall'utente stesso. La password e il codice identificativo sono personali.
Pertanto vanno osservate le seguenti misure di sicurezza:

- evitare di rendere note le password. E', in primo luogo, interesse dell'utente evitare che altri utilizzino la sua password d'accesso: infatti, dalla registrazione dell'attività effettuata dal sistema, risulterebbe a lui attribuito il trattamento effettuato da altri, con connessa responsabilità in caso di trattamenti scorretti o non autorizzati o illeciti;
- evitare di trascrivere le password su supporti agevolmente accessibili da parte di terzi;
- evitare di utilizzare codici di accesso di personale nel frattempo cessato, assente per lungo periodo o che è stato assegnato ad altra struttura o attività.

Il Preposto è supportato dal referente informatico della Struttura - in caso di entrata in servizio, cessazione, mobilità o cambio di mansioni del personale assegnatario di dotazioni informatiche - nel provvedere alla richiesta dei relativi nuovi inserimenti, delle cancellazioni o delle modifiche alle abilitazioni utente che si rendano necessarie secondo le modalità individuate con la procedura operativa per la gestione delle richieste di attività IMAC, nell'ambito del servizio di Change Management. Questa regola è valida anche se si stanno introducendo sistemi automantici di provisioning e deprovisoning delle identità digitali (IAM)

L'accesso ai dati, per ragioni di lavoro, da parte dei colleghi dell'Addetto assente, può essere facilmente ottenuto utilizzando le cartelle del disco U per tutte le attività che prevedono la collaborazione di più utenti. Nel caso, invece, di trattamenti di dati effettuati da un singolo Addetto, se il Preposto deve accedere ai dati in sua assenza, può fare richiesta all'Amministratore di sistema di essere, temporaneamente, abilitato ad accedere alla cartella che li contiene. Si rammenta che **l'Amministratore di sistema non ha modo di conoscere le password degli altri utenti** (che sono conservate sul server in forma cifrata), ma ha sempre accesso diretto e immediato a tutti i dati e può abilitare all'accesso anche altri utenti. **I dati, quindi, sono sempre reperibili anche in assenza della persona che conosce la password.**
L'utente è tenuto a:

- sostituire la password ad intervalli regolari; il sistema consente la sostituzione della password da parte dell'utente, nonché anche di impostare, per tutta la rete, un vincolo che impone, a tutti gli utenti, di cambiare le password entro periodi prestabiliti, così come chiarito al precedente capitolo 3.2.1;
- rendere inaccessibile il sistema, dalla propria postazione di lavoro, ogni volta che si assenta; ciò si ottiene utilizzando la funzione di blocco *workstation* del sistema (che viene attivata premendo contemporaneamente i tasti Ctrl/Alt/Canc e cliccando sul bottone "blocca computer");
- impostare uno *screen saver* automatico protetto da password con tempo di attivazione inferiore ai 10 minuti di inattività della macchina;
- se accede alla rete, da una postazione di lavoro non assegnatagli, usare il proprio identificativo utente e la propria password e non chiedere di utilizzare la password del collega.

9.2.2 Protezione da accessi logici non autorizzati a PC non connessi alla rete

Per l'accesso logico ai PC stand-alone, cioè PC non connessi al server di rete della struttura, bisogna adottare, prima dell'inizio del trattamento dei dati personali, le seguenti misure:
se il sistema operativo lo consente, impostare password e user-id per l'accesso logico al PC, che vanno fornite a ciascun Addetto.

9.2.3 Protezione da accessi logici, non autorizzati, agli applicativi

L'accesso logico alla posta elettronica, e ad altri programmi applicativi, può essere protetto da parola chiave, associata o meno ad un user-id. Per quanto riguarda gli applicativi, vanno osservate le seguenti disposizioni:

- le applicazioni che trattano dati personali, devono essere protette con una specifica password di accesso all'applicazione stessa, oltre alla parola chiave di accesso al sistema;
- la password e l'eventuale codice identificativo sono personali;
- se necessario, la creazione, la modificazione e la cancellazione delle abilitazioni vengono richieste, dal Preposto, secondo le modalità individuate con la procedura operativa per la gestione delle richieste di attività IMAC, nell'ambito del servizio di Change Management.

9.2.4 Protezione dai virus

I PC connessi in rete sono protetti da un prodotto antivirus, installato e connesso ai sistemi server, con aggiornamento periodico automatico a carico dell'Amministratore di sistema (Trentino Digitale S.p.a. nel caso dei PC registrati nell'inventario centralizzato).

9.2.5 Protezione dal rischio di perdita accidentale dei dati

Per i dati contenuti nei dischi di rete, viene effettuato un *backup,* programmato automaticamente dal sistema server durante la notte, su apposite cassette da sostituire giornalmente.
Per i dati contenuti nei dischi installati fisicamente sul PC (C:\ e D:\) è necessario, invece, che ciascun operatore provveda a periodici backup dei dati, su supporti magnetici, e alla conservazione dei supporti stessi nel rispetto delle disposizioni individuate al paragrafo 9.5 *Misure di sicurezza relative ai supporti di memorizzazione*.
Si consiglia, comunque, di utilizzare i dischi del PC, come sistema di memorizzazione dei dati, solo quando non sono disponibili unità di rete, mentre la memorizzazione sulle unità di rete messe a disposizione dal server, **costituisce la regola**.

9.2.6 Accesso ai dati in assenza dell'Addetto

Qualora, in caso di assenza dell'Addetto assegnatario della dotazione informatica, ovvero della casella di posta elettronica, si renda necessario, per ragioni improrogabili, l'utilizzo di dati accessibili in via esclusiva con i suoi codici di accesso, si devono rispettare le seguenti regole:
Procedura operativa per l'accesso, in assenza dell'Addetto, a dati presenti su server, PC o casella di posta elettronica

A. Premessa

In merito all'accesso a dati memorizzati sul server, si rammenta che:
(a1) per il salvataggio dei dati/documenti comuni della Struttura, che devono essere accessibili a più utenti, è opportuno che vengano utilizzate cartelle collocate su dischi di rete del server dipartimentale, opportunamente condivise e protette, e accessibili a più di un soggetto.
(a2) allo stesso modo, per quanto riguarda le caselle di posta elettronica, si consiglia la creazione e l'utilizzo di caselle di posta di Struttura, opportunamente condivise e protette, e accessibili a più di un soggetto, per le comunicazioni di lavoro che possono necessitare di una consultazione da parte di più utenti.

B. Regole per l'accesso ai dati di un utente

Qualora si possa prevedere con anticipo l'assenza di un Addetto, la quale, a sua volta, impedisca l'accesso a dati, o e-mail, di interesse per la Struttura, è possibile attuare procedure preventive che permettano l'accesso alle informazioni anche nel caso di irreperibilità dell'Addetto stesso.
Di norma, nei dischi in locale (es. disco C: o D:), non dovrebbero transitare dati; nel caso in cui sulle unità C o D si trovino dei dati, i medesimi devono essere copiati, su una cartella, in un disco di rete accessibile a più utenti autorizzati.
Per l'accesso alla casella di posta, l'Addetto ha la possibilità di effettuare una "delega", per l'accesso alla propria casella e-mail da parte di altri utenti. La delega deve essere impostata, direttamente, dall'utente titolare della casella.

C. Caso residuale: come fare se si deve comunque accedere a dati di un utente in sua assenza

Premesso che non è consentito l'utilizzo dei codici di accesso di personale assente, cessato o assegnato ad altra Struttura, qualora, malgrado gli accorgimenti sopra descritti, ci si trovi nelle condizioni di dover accedere ai dati in assenza dell'Addetto, è possibile adottare la procedura descritta in seguito. Si rammenta che l'accesso è consentito solo se sussistono le seguenti condizioni: improrogabile necessità di accedere ai dati, per ragioni di servizio; accertata impossibilità, o notevole difficoltà, di raggiungere l'utente; comunicazione, al dipendente assente, da parte del Preposto, dell'accesso alle sue risorse.

C1. Accesso a dati presenti su server, o PC, in assenza dell'Addetto quale unico utente del permesso che può accedere alla cartella.

Qualora sussista la necessità di accedere a dati contenuti in una cartella protetta, presente sul server, e gli Addetti abilitati all'accesso siano irreperibili, il Preposto può chiedere che il proprio account e/o quello di altri Addetti siano abilitati all'accesso.
Se i dati, a cui si intende accedere, sono contenuti su una porzione di disco privato di un utente (es disco Y:\ o cartella "Documenti" in locale sul PC) e l'utente abilitato all'accesso sia irreperibile, il Preposto può chiedere che i dati di interesse siano copiati in una cartella sul server e che il proprio account e/o quello di altri Addetti siano abilitati all'accesso a tale cartella.
La richiesta deve essere inoltrata al CSD di Trentino Digitale S.p.a..

C2. Accesso, in assenza dell'Addetto, a casella di posta elettronica presente sul server.

Qualora si presenti la necessità di accedere a dati contenuti in una casella di posta elettronica, e l'Addetto (utente della casella) abilitato all'accesso sia irreperibile, il Preposto può chiedere che il proprio account e/o quello di altri Addetti siano abilitati all'accesso.
La richiesta deve essere inoltrata al CSD di Trentino Digitale S.p.a..
Le attività possono essere eseguite da remoto.

9.2.7 Procedura di ripristino password

La procedura di seguito descritta entrerà in vigore nel momento in cui sarà realizzato il relativo software; fino a tale termine, si applicherà la procedura di ripristino password disciplinata nella deliberazione della Giunta provinciale n. 232/2007 – Allegato B, che, di conseguenza, continuerà, esclusivamente per la parte specificata, ad esplicare i propri effetti.
La procedura entra in vigore entro, e non oltre, 4 mesi dalla data di pubblicazione della presente deliberazione.
Gli accessi alle applicazioni informatiche, della Provincia autonoma di Trento, sono protetti da password. Per garantire un adeguato livello di sicurezza, le credenziali di accesso sono protette nei modi seguenti: a) dopo 6 mesi di mancato utilizzo, scadono; b) dopo 7 tentativi errati, vengono bloccate per un'ora.
Tutte le attuali applicazioni informatiche dovranno essere adeguate a quanto sopra citato e se ciò non sarà possibile, a causa della tecnologia obsoleta con la quale sono realizzate, dovranno essere implementate tutte le misure di sicurezza necessarie per ottenere un elevato livello di sicurezza.
Al fine di ripristinare l'accesso alle applicazioni, nelle ipotesi in cui le credenziali siano scadute, bloccate o smarrite, è utilizzabile una procedura di riattivazione che, conformemente alla normativa vigente in materia di sicurezza, risulta caratterizzata da tempi minimi di ripristino.
La procedura assicura che la password sia consegnata esclusivamente all'utente, e che venga, sempre, notificato, sulla casella di posta elettronica istituzionale personale, l'avvio della procedura di ripristino.
Ciascuna applicazione informatica, al primo accesso con la password fornita in seguito al processo di ripristino, richiede all'utente di inserirne una nuova. L'applicazione verifica anche che siano rispettati i requisiti minimi di complessità.
Il procedimento, le basi dati, gli operatori e quanto necessario per soddisfare la richiesta di ripristino, verranno di seguito indicati come "sistema".
Il processo di ripristino della password ha inizio con una richiesta effettuata attraverso il portale per la gestione delle richieste informatiche (di seguito indicato come "portale"), previa autenticazione da parte dei seguenti soggetti:

- utente destinatario della richiesta;
- referente informatico della Struttura a cui appartiene l'utente;
- Consumer Service Desk;

- gruppo di supporto dell'applicazione.

In tutti i casi in cui richiedente e destinatario della richiesta non coincidono, viene inviata una mail di notifica alla casella istituzionale dell'utente o a quella personale, se presente nel sistema.
Per la comunicazione della nuova password, il sistema propone, al richiedente, una lista di canali selezionabili in ordine di priorità:

- casella di posta nominativa istituzionale del destinatario della richiesta, se non è il sistema da ripristinare
- SMS al cellulare aziendale del destinatario della richiesta
- casella di posta personale del destinatario della richiesta, se preventivamente fornita su base volontaria
- SMS al cellulare personale del destinatario della richiesta, se preventivamente fornito su base volontaria
- lettera in busta chiusa riservata all'indirizzo del destinatario della richiesta

La sequenza descritta non rappresenta una mera formalità, ma serve a implementare la sicurezza, in quanto predisposta per garantire, all'Amministratore di sistema, che la richiesta di ripristino password provenga da chi è effettivamente legittimato al trattamento dei dati. Si sono, infatti, verificati casi in cui le violazioni di sistemi protetti sono state ottenute da malintenzionati che si spacciavano per altre persone (dichiarando, al telefono, di aver smarrito la password e ottenendone il ripristino).

Inoltre, solo per il reset della password della posta elettronica, in alternativa, può essere utilizzato, se attivato dall'Amministrazione, il canale messo a disposizione dal sistema di posta, che risulta utilizzabile solo nel caso in cui l'utente abbia fornito, preventivamente, una casella di posta personale e/o un numero di cellulare.

Dati archiviati

Nel portale, a cura dell'utente o del sistema, vengono memorizzate le seguenti informazioni:

a) Nome e Cognome;
b) Matricola;
c) Indirizzo della casella di posta elettronica personale istituzionale (nome.cognome@provincia.tn.it);
d) Indirizzo postale del luogo di lavoro;
e) Indirizzo postale della segreteria di riferimento;
f) Numero di cellulare di servizio (se disponibile);
g) Indirizzo della casella di posta personale (facoltativo, a discrezione dell'utente);
h) Numero di cellulare personale (facoltativo, a discrezione dell'utente).

Aggiornamento dei dati da parte dell'utente

Per accedere alle funzioni di aggiornamento dei dati del portale, l'utente deve essere autenticato: l'autenticazione avviene attraverso l'accesso alla propria postazione di lavoro o tramite apposita procedura.
I dati personali, relativi all'indirizzo della casella di posta elettronica personale e al numero di cellulare personale, possono essere inseriti ed aggiornati dall'utente. Gli altri dati (numero cellulare di servizio, casella personale istituzionale) sono inseriti e aggiornabili, attraverso il sistema, automaticamente.

Ad ogni inserimento ed aggiornamento di dati, da parte dell'utente, il sistema ne controlla e ne verifica la correttezza e la validità.
I dati sono modificabili dall'utente, direttamente o tramite richiesta al sistema, solamente se non vi sono richieste di ripristino password pendenti.
Le modifiche dei dati, e le richieste di ripristino password, vengono notificate all'utente, riportando le informazioni indicate nel registro degli accessi sul portale descritto in seguito.

Registro delle attività nel portale delle password

Il portale, previa autenticazione, consente di controllare le richieste di ripristino password.
Il registro, per ogni richiesta di ripristino password e ogni richiesta di aggiornamento dei dati, contiene la data e l'ora della richiesta, l'indirizzo IP dal quale è stata inoltrata, gli estremi dell'utente richiedente, la tipologia, l'applicazione di riferimento.

9.3 Modalità e procedure, relative alla salvaguardia dei dati personali memorizzati sui pc, in caso di dismissione e/o sostituzione delle apparecchiature

9.3.1 Introduzione

I tradizionali supporti di memorizzazione (hard disk, supporti USB, altro), utilizzati nella quotidiana attività lavorativa, contengono un'enorme quantità di dati riservati.

I frequenti refresh tecnologici, favoriti da un sempre minor costo dell'hardware, richiedono che sia gli strumenti di memorizzazione (es. gli hard disk) che qualunque oggetto li contenga (es. i PC), vengano movimentati, con la dovuta cautela, soprattutto quando vengono ceduti per un qualsiasi motivo.

Gli utenti, normalmente, danno per scontato che i dati cancellati tramite sistema operativo, o contenuti su supporti danneggiati, non siano più disponibili per successivi utilizzi. La rapida evoluzione tecnologica degli ultimi anni ha permesso, purtroppo, lo sviluppo di strumenti software che consentono un agevole recupero dei dati, siano questi cancellati in maniera tradizionale o memorizzati su supporti danneggiati, anche da parte di utenti non particolarmente esperti e con costi molto contenuti.

Il metodo più efficace, per preservare la riservatezza delle informazioni memorizzate su supporti, è la distruzione fisica degli stessi. Tale metodo è particolarmente indicato per gli strumenti che, per loro natura, non possono essere riutilizzati (es. CD e/o DVD), mentre, con riferimento ai supporti riutilizzabili (es. hard disk, supporti esterni, chiavette USB, nastri di backup etc.), è necessario considerare l'elevato costo di un approccio di questo tipo.

L'alternativa più frequentemente utilizzata, rispetto alla distruzione fisica dei supporti, è quella della completa riscrittura mediante l'utilizzo di appositi software. Attraverso tale operazione, infatti, i dati precedentemente memorizzati non potranno essere più reperibili.

9.3.2 Dismissione della postazione di lavoro

Nell'ipotesi in cui venga sostituita la postazione di lavoro, il disco rigido verrà formattato dai tecnici incaricati da Trentino Digitale S.p.a., con un processo che garantisce l'irrecuperabilità dei dati precedentemente memorizzati. Sulla base di quanto sopra esposto, costituisce responsabilità dell'utente assegnatario provvedere a copiare tutti i dati che devono essere salvaguardati, nei percorsi standard (cartella Documenti), affinché il tecnico incaricato possa provvedere al loro riversamento sulla nuova postazione. I dati non riversati non potranno in alcun modo essere recuperati.

9.3.3 Sostituzione dell'hard disk

Nel caso di sostituzione del disco rigido della postazione di lavoro, da parte dei tecnici incaricati da Trentino Digitale S.p.a., il contenuto sarà cancellato mediante un processo che garantisce l'irrecuperabilità dei dati precedentemente memorizzati. Oppure, nel caso non se ne preveda il riutilizzo, l'hard disk verrà distrutto fisicamente.

Per eventuali postazioni, non direttamente gestite da Trentino Digitale S.p.a., per le quali la sostituzione dell'hard disk non viene effettuata da personale incaricato dalla Società stessa, sarà necessario richiedere un intervento congiunto, per garantire la cancellazione irreversibile di tutti i dati, prima che il disco sostituito venga consegnato al tecnico esterno.

Sulla base di quanto specificato, costituisce precisa responsabilità dell'utente assegnatario provvedere ad indicare, al tecnico incaricato, tutti i dati che devono essere copiati sul nuovo supporto, affinché il medesimo possa provvedere al loro riversamento.

I dati non riversati non potranno in alcun modo essere recuperati.

9.4 Misure di sicurezza relative ai pc portatili

9.4.1 Misure di sicurezza logistiche

9.4.1.1 Protezione da accesso fisico non autorizzato e dal furto

Il personale che ha in consegna un PC portatile è tenuto a:
- evitare di lasciare incustodito il portatile per evitare il rischio di furto;
- custodire i portatili negli armadi muniti di serratura;
- escludere l'accesso ai dati da parte di soggetti non autorizzati al trattamento, evitando, così, che tali dati giungano a conoscenza di terzi;
- evitare, ove non strettamente necessario per lo svolgimento dei compiti affidati, la connessione del portatile a reti che non siano quella provinciale.

9.4.2 Misure di sicurezza tecniche, informatiche e procedurali

9.4.2.1 Protezione da accesso logico non autorizzato

Si richiamano, in quanto compatibili con le caratteristiche tecniche del PC portatile e con le esigenze organizzative, le misure previste per l'accesso logico alle postazioni di lavoro fisse (user-id, password, comunicazione della password al custode, screen saver…).

9.4.2.2 Protezione dai virus

Per ridurre al minimo il pericolo di perdite di dati a causa di virus informatici, è necessario verificare che sia installato un prodotto antivirus ad hoc: per risultare efficace nel tempo, deve essere aggiornato, periodicamente, secondo le modalità richieste dal prodotto stesso.

9.4.2.3 Protezione dai malintenzionati

I PC portatili, quando collegati a rete diversa da Telpat, o connessi a Internet, tramite un provider diverso da Trentino Digitale S.p.a., non usufruiscono della protezione effettuata tramite *firewall* gestito da Trentino Digitale S.p.a. stessa.
Pertanto, a fronte del pericolo di attacchi esterni da parte di malintenzionati, vanno adottate le seguenti cautele:
- evitare, ove non strettamente necessario per lo svolgimento dei compiti affidati, la connessione del portatile a reti che non siano quella provinciale
- ove sia necessario collegarsi a reti, concordare idonee misure di sicurezza con la Struttura competente in materia di sicurezza informatica.

9.4.2.4 Protezione dal rischio di perdita accidentale dei dati

Nel caso non sia possibile connettere il portatile alla rete dell'ufficio, il personale che lo ha in uso è tenuto a:
- provvedere a periodici backup, dei dati contenuti nel disco fisso del portatile, su supporti magnetici;
- custodire i supporti di backup osservando le precauzioni individuate nel paragrafo 9.5 “Misure di sicurezza relative ai supporti di memorizzazione”.

9.5 Misure di sicurezza relative ai supporti di memorizzazione

9.5.1 Misure di sicurezza logistiche

Nell’uso e nella conservazione dei supporti di memorizzazione devono essere rispettate le misure necessarie a ridurre al minimo i rischi di:
- accesso fisico non autorizzato;
- furto e manomissione dei dati da parte di malintenzionati;
- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

Sono necessari, inoltre, gli ulteriori accorgimenti, di seguito riportati, derivanti dalle specifiche caratteristiche di tali supporti.

Riutilizzo

I supporti rimovibili contenenti dati appartenenti a particolari categorie o relativi a condanne penali e reati, se non utilizzati, sono distrutti, o resi inutilizzabili, ovvero possono essere riutilizzati da altri Addetti, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente contenute, non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Si riportano, di seguito, le indicazioni operative da seguire, relative ad alcuni supporti, nel caso in cui gli stessi siano consegnati a terzi:
- supporti rimovibili: prima di essere consegnati a terzi, debbono essere sottoposti ad una operazione di cancellazione delle informazioni precedentemente contenute, attraverso l'apposito comando di formattazione completa del supporto e utilizzando software per la cancellazione sicura dei dati;
- hard disk: prima di essere consegnato a terzi, deve essere sottoposto ad una operazione di cancellazione delle informazioni precedentemente contenute, tramite apposita procedura;
  nel caso in cui, a seguito di intervento tecnico, si ravvisi la necessità di sostituire l’hard disk, è necessario procedere alla cancellazione dei dati dall'hard disk sostituito; si ricorda che l’hard disk potrebbe costituire un mezzo di esportazione illegittimo di dati personali, qualora gli stessi fossero recuperati da personale non autorizzato;
- nel caso in cui i supporti contenenti dati personali non siano destinati al riutilizzo, essi debbono essere fisicamente distrutti mediante rottura.

9.6. Regole per l’utilizzo delle dotazioni informatiche

9.6.1 Uso corretto

Tutti i beni che la Provincia autonoma di Trento mette a disposizione, per lo svolgimento dell’attività lavorativa, restano nella disponibilità esclusiva della stessa. Pertanto, devono essere utilizzati, da parte di coloro che operano a qualunque livello e con qualsiasi rapporto, in maniera adeguata, anche al fine di evitare comportamenti potenzialmente pericolosi per la sicurezza del sistema informativo, derivanti da conoscenza non adeguata o incompleta, ed in conformità alle mansioni attribuite, dal contratto di lavoro, all’utente. Tutti gli utenti, che accedono alle reti LAN della Provincia, vengono automaticamente abilitati all’utilizzo di Internet ed è facoltà dei

responsabili delle Strutture di appartenenza chiedere di limitare l'accesso a determinati utenti e a determinate categorie di siti.

Tutti i soggetti, che utilizzano gli strumenti informatici messi a disposizione dalla Provincia per lo svolgimento dell'attività lavorativa, devono:

a) adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la confidenzialità dei dati personali e di quelli che possono fornire indicazioni utili ad un eventuale attaccante dei sistemi informativi (per es. dati relativi ad incidenti di sicurezza pregressi, alla tipologia di rete, alla configurazione dei software, all'ubicazione dell'hardware, al personale Preposto alla gestione ed alla sicurezza dei sistemi);

b) utilizzare, sulle postazioni di lavoro, esclusivamente il software autorizzato e fornito dalla Provincia: richiedere eventuale software aggiuntivo, rispetto all'installazione standard, al proprio referente informatico;

c) in caso di telelavoro, durante l'attività lavorativa, utilizzare la postazione di lavoro fornita esclusivamente per motivi inerenti all'attività lavorativa, senza manomettere, in alcun modo, gli apparati e la configurazione della postazione stessa, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi. Internet può, comunque, essere utilizzato, anche per motivi personali, purchè nei limiti specificati dal Disciplinare appovato con delibera della Giunta provinciale n. 1037/2010. Se si utilizzano dispositivi mobili per il telelavoro, collegare gli stessi, alla LAN della Provincia, almeno una volta ogni 7 giorni per l'aggiornamento automatico delle patch di sicurezza;

d) utilizzare gli strumenti di telefonia, sia fissa che mobile, per lo svolgimento dell'attività lavorativa ed in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi. Per tutto quanto non specificato, ci si dovrà attenere al Disciplinare, approvato con deliberazione della Giunta provinciale n. 1037/2010 o suo successivo aggiornamento.

9.6.2 Uso non consentito delle dotazioni informatiche e telefoniche

Le seguenti attività sono proibite:

a) inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti. Tali segnalazioni vanno inviate solo all'assistenza tecnica, all'indirizzo sicurezza@infotn.it oppure analisi_spam@infotn.it.;

b) rimuovere il programma antivirus installato sulla postazione di lavoro;

c) lasciare incustoditi i dispositivi mobili;

d) aprire allegati di posta elettronica, dal mittente e/o dall'oggetto sospetti, per prevenire i rischi causati da software nocivi (per es. virus, worm, spyware, ecc.). E' necessario cancellare immediatamente tali messaggi e, in caso di dubbio, contattare l'indirizzo di posta dedicato alle problematiche di sicurezza **(**sicurezza@infotn.it **oppure analisi_spam@infotn.it)**;

e) effettuare copie non autorizzate, di materiale coperto da copyright, compresi digitalizzazione e distribuzione di foto da riviste, libri o altre fonti protette da copyright; musica coperta da copyright;

f) eseguire attività di Port Scanning o Security Scanning;

g) eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'utente;

h) aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete o account;

i) interferire o bloccare l'operatività di qualunque utente (es. Denial of Service Attack) ivi compreso l'utilizzo di qualunque programma/script/comando o l'invio di un messaggio, sia localmente sia via Internet/Intranet/Extranet, con l'intento di interferire o disabilitare una qualunque connessione di altri utenti;

j) inviare messaggi di posta elettronica non desiderati, o richiesti, ivi inclusa la spedizione di qualunque informazione pubblicitaria, a soggetti che non abbiano specificatamente richiesto tali informazioni o l'inoltro di email appartenenti a catene o similari (Spam);

k) utilizzare intestazioni delle email non autorizzate.

La lista sopra riportata non deve essere considerata esaustiva, ma intende fornire un quadro di massima delle attività che ricadono nella categoria di un utilizzo non accettabile.

9.6.3 Eccezioni agli usi non consentiti

Gli utenti possono essere dispensati, da una o più delle restrizioni previste dal Disciplinare approvato con deliberazione della Giunta provinciale n.1037/2010, nel caso in cui tali limiti compromettano lo svolgimento di attività che rientrino tra quelle previste, esplicitamente, dalle loro mansioni lavorative, e siano pertanto ufficialmente autorizzate dai responsabili di Struttura.

9.7 Regole per la configurazione delle postazioni di lavoro della Provincia

9.7.1 Premessa

Il contenuto del presente paragrafo è giustificato dal fatto che alcuni utenti sono Amministratori del proprio posto di lavoro e, quindi, sono in grado di modificare la configurazione standard di seguito descritta e predisposta da Trentino Digitale S.p.a..

Nel momento in cui le postazioni di lavoro sono collegate in rete, le medesime divengono, automaticamente, vulnerabili in seguito ad un attacco, ai virus, agli errori umani (accidentali o dolosi) etc.. A causa di tale circostanza, un utente sufficientemente motivato, e con adeguate conoscenze tecniche, è in grado di individuare eventuali errori e/o dimenticanze, nella configurazione di un sistema, e metterne a rischio la riservatezza dei dati contenuti, nel caso migliore, o addirittura le funzionalità dello stesso.

La sicurezza di un sistema non può essere, dunque, un'attività occasionale, ma deve essere parte integrante del modo di lavorare, poichè, in ogni istante, occorre cercare di mettere al riparo dalle minacce esistenti utenti, dati, transazioni, ecc..

Per tale motivo, all'atto della configurazione di un sistema in rete, è compito dell'Amministratore implementare, con ragionevoli misure di sicurezza, la difesa dello stesso: la loro applicazione limiterà l'esposizione del sistema ai rischi esistenti ovvero ne ridurrà la vulnerabilità.

9.7.2 Configurazione Standard

Il sistema operativo, autorizzato sulle postazioni di lavoro in dotazione ai dipendenti della Provincia, è la versione più aggiornata di Microsoft Windows, ovvero il sistema operativo più adeguato allo svolgimento delle attività lavorative.
Nel caso di postazioni di lavoro con sistema operativo Microsoft Windows, tutti i file del sistema operativo, e tutti i programmi, durante il processo di installazione e configurazione, dovranno essere memorizzati sulla partizione principale "C"; le informazioni personali degli utenti utilizzatori dovranno essere allocate, nella apposita cartella utente, all'interno della cartella "Utenti".

9.7.3 Regole per gli utenti amministratori della propria postazione di lavoro

Nel rispetto della Circolare AGID, gli utenti, su richiesta motivata del responsabile della Struttura, possono diventare Amministratori del proprio posto di lavoro. Si ricorda ai Preposti, cui compete tale concessione, che l'opportunità di essere Amministratore del proprio PC, da un lato, permettendo di operare sulla configurazione della propria macchina, aumenta la cultura informatica del personale, dall'altro, però, comporta un aumento dei costi di manutenzione dovuti ad errori di utenti non professionali. Si raccomanda, quindi, ai responsabili di Struttura, di valutare attentamente le caratteristiche individuali degli utenti ai quali si decide di concedere i privilegi di Amministratore della propria postazione di lavoro.

La richiesta sarà analizzata dalla Struttura competente in materia di sicurezza informatica e potrà essere respinta se non debitamente motivata.

Gli utenti, ai quali è stato concesso di essere Amministratore della propria postazione di lavoro, sono comunque tenuti a rispettare le seguenti regole:

1. non istallare software non regolarmente licenziati;
2. non disabilitare il sistema di antivirus;
3. non bloccare gli aggiornamenti di sicurezza del software installato;
4. nel caso di interventi tecnici, segnalare l'installazione di software licenziati non previsti dalla configurazione standard.

Qualora fossero violate le regole 1, 2, 3 sarà revocato il privilegio di Amministratore della propria postazione di lavoro, segnalando la violazione al Servizio per il Personale.

L'uso appropriato dei privilegi di Amministratore locale della propria postazione di lavoro impone le seguenti regole:

- limitare i privilegi di Amministratore ai soli utenti che abbiano competenze adeguate e necessità operative;
- mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata;
- gestire l'inventario delle utenze amministrative.

9.7.4 Regole per il collegamento di dispositivi gestiti direttamente dall'utente

Nel caso in cui sussista la necessità di configurare, nella rete provinciale, un qualsiasi dispositivo con il corrispondente indirizzo IP, devono essere rispettate le seguenti indicazioni:

- inventariare il dispositivo che si deve collegare alla rete, individuando obbligatoriamente il titolare della risorsa;
- aggiornare l'inventario quando vengono collegati in rete nuovi dispositivi e il corrispondente indirizzo IP;
- i dispositivi collegati alla rete devono utilizzare configurazioni sicure standanrd per la protezione dei sistemi operativi;
- i sistemi operativi dei dispositivi, quando possibile, devono essere sempre aggiornati all'ultima versione disponibile, in particolare devono essere sempre installate le patch di sicurezza rese disponibili;
- il dispositivo, collegato alla rete, deve deve essere dotato di antivirus sempre aggiornato; in dettaglio è consigliabile collegarsi al repository messo a disposizione da Trentino Digitale S.p.a..

Per motivi di sicurezza, sul dispositivo possono essere eseguiti appositi controlli per verificare la presenza di eventuali vulnerabilità e, se necessario, il dispositivo può essere disconnesso dalla rete.

10. MISURE DI SICUREZZA RELATIVE ALLE AULE CORSI

Le aule dove si tengono corsi di formazione, nelle quali siano presenti postazioni informatiche connesse al server di una Struttura, oppure archivi cartacei contenenti dati personali, vanno protette con adeguate misure di sicurezza. Le misure logistiche e quelle di difesa da attacchi virus devono essere applicate, in generale, a tutte le aule corsi nelle quali siano presenti dotazioni informatiche, anche non connesse al server di una Struttura (ad es. stazioni stand-alone o stazioni collegate in rete tra loro o ad un server riservato alla sola aula).

10.1 Misure di sicurezza logistiche

10.1.1 Protezione dall'accesso fisico non autorizzato

In primo luogo, devono essere adottate le seguenti misure:

- le aule corsi, quando non vengono utilizzate, come ad esempio durante la pausa pranzo, devono essere chiuse a chiave;
- le chiavi delle aule corsi sono depositate presso il personale incaricato della custodia dal responsabile della Struttura competente per la gestione dell'aula;
- le aule vengono aperte e chiuse da personale dell'Amministrazione provinciale: non è ammessa la consegna di chiavi a personale esterno;
- il docente, o eventuale altro personale di sorveglianza, deve essere sempre presente in aula in modo da poter contrastare eventuali tentativi di danneggiamento delle dotazioni informatiche;
- l'accesso alle aule, da parte di personale esterno all'Amministrazione, deve essere appositamente autorizzato.

10.2 Misure di sicurezza tecniche, informatiche e procedurali

10.2.1 Protezione dall'accesso logico al sistema non autorizzato

Il docente, o eventuale personale di sorveglianza, deve essere sempre presente in aula, in modo da poter contrastare eventuali tentativi, non autorizzati, di accesso logico ai sistemi. Conseguentemente, devono essere adottate le seguenti misure:

- ove il software di sistema lo consenta, è fatto obbligo di attivare la funzione di screen saver con parola chiave (con tempo di attivazione inferiore ai 5 minuti) per evitare possibili accessi non autorizzati alla rete.

10.2.2 Protezione dai virus

Le postazioni informatiche dell'aula, connesse in rete, sono protette da un prodotto antivirus installato sul server, con aggiornamento periodico automatico via Internet a carico dell'Amministratore di sistema.
Sulle postazioni non connesse, al fine di evitare la propagazione dei virus, deve essere installato un prodotto antivirus ad hoc, aggiornato periodicamente, secondo le modalità richieste dal prodotto stesso. L'aggiornamento è a carico dell'Amministratore di sistema (cioè Trentino Digitale S.p.a. nel caso dei pc registrati nell'inventario centralizzato).

10.2.3 Protezione dai malintenzionati

Le postazioni di lavoro delle aule corsi, collegate alla rete Telpat, sono protette tramite *firewall* gestito da Trentino Digitale S.p.a.. La difesa dagli attacchi di questo tipo è comunque assicurata solo se viene data puntuale applicazione a tutto il complesso delle regole di sicurezza comprese nel presente documento.

11. MISURE DI SICUREZZA RELATIVE A INTERNET

11.1 Premessa

L'utilizzo di una connessione ad Internet, attraverso un *provider* diverso da Trentino Digitale S.p.a., espone il pc utilizzato ai rischi normalmente presenti nel corso di una connessione ad Internet, in assenza della protezione garantita da un *firewall*.
Inoltre:

- l'eventuale attacco alla macchina, nel corso della navigazione non protetta, diventa un fattore di rischio per l'intera rete provinciale;
- sia l'accesso a siti "impropri", che lo scaricamento di file non autorizzati, in alcuni casi possono essere illegali e puniti dalla legge penale (oltre ad essere in contrasto con il codice di disciplina del dipendente provinciale);
- l'utilizzo della connessione Internet della Provincia, per finalità non riconducibili all'attività di lavoro, anche se non produce un costo diretto, **può diventare causa di sovraccarico della linea** e può portare a un deterioramento della velocità della connessione per tutti gli utenti;
- le informazioni presenti su siti Internet non connessi a istituzioni ben conosciute, possono essere **non accurate**, **non valide o deliberatamente false**: ogni decisione basata su di esse deve essere valutata adeguatamente;
- qualora il collegamento, alla rete Internet, avvenga al di fuori di Telpat (ad es. tramite PC portatile), ogni macchina che può accedere a Internet (o il server, se gli elaboratori sono in rete) va protetta da un antivirus aggiornato; non aggiornarlo, può essere più pericoloso che non averlo: si crea una falsa sicurezza.

> I messaggi di posta elettronica, dei quali non si conosce il mittente, vanno trattati con la massima circospezione. **Non bisogna mai cliccare sugli eventuali allegati senza riflettere**; si tenga presente che i danni, per virus ricevuti attraverso la posta elettronica, rappresentano, da soli, la grande maggioranza delle cause di eventi dannosi, collegati a virus informatici, all'interno delle reti aziendali.

Anche in presenza di un utente conosciuto, è meglio riflettere sul contesto del messaggio per verificare se l'allegato è, in qualche modo, connesso con il proprio lavoro (e quindi viene effettivamente dal mittente indicato).

11.2 Regole per l'utilizzo della rete Internet

Non è pensabile, al giorno d'oggi, lavorare senza l'ausilio di Internet ma, allo stesso tempo, occorre evitare, e prevenire, comportamenti anomali ovvero garantire un uso appropriato dello strumento. La rete, infatti, permette di accedere a moltissimi siti, contenenti informazioni più o meno lecite, che possono anche contenere virus e/o software malevoli, creati per interrompere, distruggere e/o limitare il funzionamento degli applicativi, degli apparati hardware o delle comunicazioni di rete. Purtroppo, anche a fronte di una semplice ed innocua ricerca in Internet, non è sempre facile evitare di imbattersi, almeno una volta, in siti web non conformi o contenenti informazioni inadeguate.

La delibera del Garante Privacy n. 13/2007, emanata in data 01/03/2007, ha disposto una serie di prescrizioni ed adempimenti, relativamente all'accesso ai dati del personale dipendente da parte del

datore di lavoro, riferendosi specificatamente anche alle informazioni desumibili dall'analisi dei log del traffico web effettuato dalle postazioni aziendali.

Nello specifico, pur dettando delle linee guida molto stringenti a protezione dei dati personali dei dipendenti, il Garante Privacy ha altresì riconosciuto la necessità che il datore di lavoro, ovvero il Titolare del trattamento, adotti opportune misure, per ridurre il rischio di usi impropri della connessione aziendale ad Internet. Ciò al fine di ridurre i controlli successivi sui lavoratori, e di predisporre opportune procedure per disciplinare l'accesso alle informazioni del dipendente (limitatamente alla casella di posta elettronica di lavoro e alle risorse di rete) in caso di improvvisa e/o prolungata assenza dell'Addetto.

Le condizioni dettate dal Garante per garantire la liceità del trattamento, prevedono, tra l'altro, l'adozione e pubblicazione di un disciplinare interno, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica, nonché l'adozione delle necessarie misure, di tipo organizzativo e tecnologico, per offrire, all'utente, soluzioni alternative.

E', inoltre, compito del datore di lavoro informare il personale dipendente, con chiarezza e in modo dettagliato, sulla possibilità che vengano effettuati controlli e con quali modalità.

La Provincia autonoma di Trento ha provveduto a definire le modalità d'uso di Internet e posta elettronica con deliberazione della Giunta provinciale n. 1037/2010, attraverso la quale è stato adottato il "Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche."

11.2.1 Disposizioni per l'accesso a Internet

Onde limitare la necessità di controlli successivi ed in conformità a quanto disposto dal Garante Privacy, sono definite le seguenti linee guida, relativamente alla navigazione in Internet:

- le richieste di accesso, provenienti da dipendenti della Provincia a siti Internet interdetti, devono essere verificate e autorizzate dall'infrastruttura cui compete l'attività di filtro degli indirizzi Internet;
- è facoltà dei Preposti chiedere ulteriori restrizioni, o particolari concessioni, per gli utenti alle dirette dipendenze; tutti gli utenti che accedono alle reti LAN della Provincia, infatti, vengono automaticamente abilitati all'utilizzo di Internet, ma è facoltà dei responsabili delle Strutture di appartenenza chiedere che l'accesso venga circoscritto a determinati utenti e a determinate categorie di siti;
- per gli apparati di infrastruttura (server, apparati di rete etc.), per i quali si renda necessario consentire un accesso ad Internet (p.e. per l'aggiornamento del software), verranno applicate le stesse restrizioni riportate nel paragrafo 11.3.1 (Categorie interdette alla navigazione) e verranno identificati tramite il loro indirizzo IP.

11.3 Disposizioni generali per la navigazione in Internet

Gli utenti che accedono ad Internet, tramite la rete provinciale Telpat, sono tenuti a rispettare alcune norme comportamentali per un uso etico e legale della rete.

Ad integrazione di quanto riportato nel paragrafo 9.6 della presente Sezione, vengono di seguito specificati ulteriori comportamenti da evitare, poiché si pongono in contrasto con la normativa vigente:

- creare, trasmettere, pubblicare e/o archiviare qualsiasi tipo di materiale:
    - che infranga le leggi sul diritto d'autore e la proprietà intellettuale;
    - che includa contenuti che siano dannosi, minatori, molesti, offensivi, calunniosi o volgari;

  - che violi la normativa in tema di protezione dei dati personali;
  - che incoraggi il compiersi di azioni criminali;
  - che, in generale, possa arrecare danno alla Provincia;
- partecipare a forum, chat e simili se ciò non è richiesto dall'attività lavorativa;
- rimanere collegati a siti musicali, anche se contestualmente si continua la propria attività lavorativa, in particolare per periodi di tempo prolungati, in quanto ciò appesantisce il traffico della rete.

11.3.1 Categorie interdette alla navigazione

Nell'intento di prevenire comportamenti illegittimi, la Provincia ha adottato una soluzione tecnologica volta a bloccare l'accesso a determinati siti, a contenuto non pertinente alla normale attività istituzionale.
L'intervento sul traffico Internet, con modalità automatiche di filtro e inibizione, non comporta un controllo diretto o indiretto sull'attività individuale, ma semplicemente impedisce l'accesso a determinati siti non pertinenti all'attività istituzionale, così come previsto anche dal provvedimento del Garante Privacy n. 13 dell'1 marzo 2007.

Per gli utenti Telpat è inibita la navigazione sui siti che rientrano nelle seguenti macro categorie, poiché non correlate o correlabili con l'attività lavorativa:
- siti che trattano argomenti illeciti;
- siti contenenti argomenti di cattivo gusto;
- siti che trattano armi e armamenti in generale;
- siti che permettono la chat via Web;
- siti legati al gioco (giochi online, gioco d'azzardo, recensione giochi);
- siti inerenti al file sharing in generale e al peer-to-peer in particolare, salvo le eccezioni di cui punti 8A e 8C del disciplinare per l'utilizzo della rete Internet, della posta elettronica, delle attrezzature informatiche e telefoniche (Deliberazione Giunta provinciale n. 1037 del 2010);
- siti che riconoscono un corrispettivo economico legato alla navigazione;
- siti di intermediazione finanziaria e trading online;
- siti che trattano file musicali (MP3) o, più in generale, forniscono illecitamente materiale coperto dal diritto d'autore;
- siti contenenti materiale per adulti, nudità o comunque con contenuti legati al sesso (fanno eccezione i siti di natura medica e scientifica);
- siti che permettono di eludere i sistemi di controllo della navigazione, tramite l'utilizzo di proxy o l'occultamento dell'URL di destinazione/provenienza;
- siti riguardanti Hacking o pirateria informatica;
- siti collegati alle violazioni della sicurezza informatica;
- siti per lo streaming audio e video (solo per quanto riguarda siti che violano i diritti di autore);
- siti legati al razzismo, al fanatismo e all'estremismo;
- siti con contenuti violenti;
- siti che si occupano esclusivamente di pubblicità.

11.3.2 Eccezioni agli usi non consentiti

Gli utenti possono essere dispensati da una o più delle precedenti restrizioni, nel caso in cui gli accessi vietati siano pertinenti alle loro mansioni lavorative, e siano pertanto ufficialmente autorizzati.
Con riferimento alle linee telefoniche, alla posta elettronica, a Internet e agli altri beni telematici, gli utenti devono utilizzare tali strumenti nei limiti specificati dal disciplinare approvato con delibera della Giunta provinciale n. 1037/2010.

11.4 Conservazione dei log

I log del traffico Internet (ora e data, ip del client, userid, indirizzo o url di destinazione e protocollo), sono registrati e conservati da Trentino Digitale S.p.a., fornitore del servizio, nel rispetto di quanto previsto dagli articoli 132 e ss. del D. Lgs n. 196/2003 e dai relativi provvedimenti del Garante in materia di sicurezza dei dati di traffico telefonico e telematico.

12. VERIFICHE DI SICUREZZA

12.1 Premessa

Le verifiche previste in questo paragrafo consentono di monitorare la concreta attuazione delle misure di sicurezza informatica adottate dall'Amministrazione, e di effettuare il loro costante aggiornamento e adeguamento; ciò risponde all'obbligo, posto in capo a ciascun Titolare di trattamenti di dati personali, di mettere in atto le adeguate misure di sicurezza (ai sensi degli artt. 28 e 32 del Regolamento UE 2016/679) per prevenire i rischi di distruzione e di perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Pertanto, tali verifiche costituiscono esse stesse una misura di sicurezza, che, in quanto tale, è obbligatoria per la Provincia autonoma di Trento, nella sua qualità di Titolare del trattamento di dati personali.

E' bene ricordare che la sicurezza di un sistema è strettamente connessa alla sicurezza del suo anello più debole e che l'interconnettività e interdipendenza, fra le componenti di un sistema informativo, implicano che i problemi di sicurezza, su una sola di esse, propaghino i loro effetti incidendo, gravemente, sulla sicurezza del sistema nel suo complesso.

Le verifiche di sicurezza oggetto del presente capitolo **sono effettuate su tutti i sistemi attinenti ai trattamenti di competenza della Provincia.**

A tale fine i responsabili di sistemi differenti da quello della Provincia, e connessi col medesimo, dovranno sottoscrivere appositi protocolli di intesa in cui si precisa che le verifiche di sicurezza sulle strumentazioni verranno effettuate con le modalità e le procedure stabilite dal presente capitolo.

12.2 Finalità

Il presente capitolo stabilisce **le prescrizioni per lo svolgimento delle verifiche e dei controlli** finalizzati ad individuare, e possibilmente prevenire, il rischio di utilizzo improprio del Sistema informativo che gestisce i trattamenti provinciali.

Le prescrizioni in tema di controlli mirano a:

- preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni;
- garantire il rispetto di leggi e regolamenti in materia di protezione dei dati personali, in particolare degli adeguati requisiti di sicurezza richiesti dalla normativa vigente;
- proteggere la Provincia autonoma di Trento ed i suoi utenti, da attività irresponsabili o illegali, nonché preservarne la reputazione e l'immagine nei confronti dei cittadini;
- ridurre la spesa pubblica, sia rilevando eventuali danni già posti in essere, sia adottando procedure che fungano da deterrente rispetto a comportamenti impropri e potenzialmente dannosi; il mancato accertamento dei quali potrebbe comportare responsabilità patrimoniali dirette a carico dell'Amministrazione;
- ridurre i rischi di coinvolgimento dell'Amministrazione, per concorso, nel caso di illeciti, civili e penali, commessi mediante l'utilizzo improprio dei beni messi a disposizione dall'Amministrazione stessa;

- verificare la coerenza del funzionamento dei sistemi informativi con le politiche di sicurezza adottate, con gli standard nazionali e/o internazionali e le normative vigenti in materia;
- individuare gli incidenti di sicurezza (comportamenti che infrangono le politiche di sicurezza) per garantire l'affidabilità e la sicurezza della rete e dei servizi erogati e/o approfondire tutte le circostanze che emergono in seguito a segnalazioni di incidenti, in modo da evidenziare eventuali rischi ed orientare la successiva attività di prevenzione;
- proporre eventuali modifiche, o nuove implementazioni, ai sistemi di sicurezza sulla base delle verifiche effettuate.

12.3 Responsabilità della Struttura competente in materia di sicurezza informatica.

I controlli previsti nel presente provvedimento sono di pertinenza della Struttura competente in materia di sicurezza informatica, che potrà, ove ritenuto necessario od opportuno, affidarli ad altri soggetti esterni.

Qualora si renda necessario l'ausilio di persone non appartenenti alle predette Strutture, tali operatori dovranno essere, dalla stessa, preventivamente autorizzati.

12.4 Procedure per lo svolgimento dei controlli

12.4.1 Principi

Le verifiche consistono in un'attività di monitoraggio sulla conformità dei sistemi informativi, e dei comportamenti dei soggetti che, a vario titolo, li utilizzano, alle prescrizioni normative e alle regole comportamentali disposte dalla Giunta provinciale, mirando a realizzare un modello fortemente improntato alla prevenzione di disfunzioni nelle procedure che implicano un trattamento di dati personali.

Le verifiche effettuate dall'Ente devono in ogni caso rispettare i seguenti principi:

a) **necessità**: i dati trattati durante l'attività di controllo devono essere sempre e soltanto quelli strettamente necessari a perseguire le finalità di cui al paragrafo 12.2 e conservati per il tempo strettamente necessario;

b) **proporzionalità**: i controlli devono sempre essere effettuati con modalità tali da garantire, nei singoli casi, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite e specificate nel paragrafo 12.2;

c) **imparzialità**: i controlli devono essere effettuati su tutte le strumentazioni informatiche messe a disposizione dall'Amministrazione provinciale e, conseguentemente, possono coinvolgere gli utilizzatori delle stesse, a qualunque titolo ne abbiano la detenzione. L'imparzialità, inoltre, deve essere garantita mediante sistemi automatici di estrazione casuale per l'effettuazione dei controlli a campione, ed in nessun caso possono essere effettuati controlli mirati, e ripetuti, nei confronti di soggetti specifici, con finalità discriminatorie o persecutorie o volutamente sanzionatorie. I controlli puntuali possono essere effettuati soltanto sulla base di specifiche, oggettive e circostanziate segnalazioni;

d) **trasparenza**: in base a tale principio l'Amministrazione deve mettere in atto tutte le azioni necessarie per garantire la preventiva conoscenza, da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente disciplinare, della possibilità di verifiche da parte del Titolare. Devono, pertanto, essere informati dei possibili controlli i soggetti che operano, a qualunque titolo e con qualunque rapporto, per conto della Provincia, tra cui, in particolare, quelli che intrattengono, con lo stesso, un rapporto di lavoro (subordinato (di qualsiasi tipologia) o autonomo);

e) **protezione dei dati personali**: i controlli devono essere effettuati, in ogni caso, rispettando la dignità e la libertà personale dei soggetti che ne risulteranno assoggettati, garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati devono essere conosciuti soltanto dai soggetti preventivamente designati quali Preposti e Addetti al trattamento.

12.4.2 Modalità

In ragione della complessità organizzativa della Provincia autonoma di Trento e della peculiarità della materia, che richiede particolari competenze professionali di carattere spiccatamente tecnico, si reputa opportuno individuare **un'articolazione organizzativa con la specifica responsabilità di sensibilizzare, coordinare, vigilare e dare attuazione agli obblighi in tema di sicurezza informatica**, nei modi di seguito specificati:

- definire idonee misure di sicurezza informatica da adottare nel trattamento di dati personali (con particolare riferimento a quelli di cui agli artt. 9 e 10 del Regolamento UE 2016/679), effettuato tramite l'impiego di strumenti elettronici;

- definire un'architettura di sicurezza che soddisfi i requisiti di cui sopra, con particolare riferimento alla armonizzazione delle misure di sicurezza con le architetture informatiche esistenti od in corso di implementazione;

- collaborare, con il Titolare, per definire linee guida in materia di protezione dei dati personali relativamente alla sicurezza informatica;

- individuare misure idonee, da osservare nell'esecuzione dei trattamenti dei dati personali, aggiornandole in relazione all'evoluzione della tecnica, della normativa, dell'esperienza e dei costi, segnalando eventuali problemi rilevati, in prima istanza, ai Preposti dei trattamenti di dati personali e, in ultima istanza, al Titolare;

- curare la redazione di disciplinari tecnici, includendo negli stessi eventuali forme di controllo, in materia di sistemi informativi e promuovendone l'aggiornamento ogni qualvolta l'evoluzione tecnica o normativa lo renda opportuno;

- ogni qualvolta venga avvertito un problema di sicurezza informatica, attivarsi per:
  - verificare il rispetto delle misure di sicurezza informatica;
  - individuare, se necessario, altre misure idonee al miglioramento della sicurezza informatica dei trattamenti dei dati personali;
  - inviare opportuna segnalazione, in prima istanza, ai Preposti e, in ultima istanza, al Titolare, affinché pongano in essere le misure necessarie per garantire la sicurezza dei dati trattati con strumenti elettronici;

- vigilare, per conto del Titolare ed avvalendosi ove ritenuto necessario di soggetti esterni, sulla puntuale osservanza delle vigenti disposizioni (e delle istruzioni fornite dal Titolare) in materia di trattamento, relativamente al profilo della sicurezza informatica, segnalando eventuali problemi rilevati, in prima istanza, ai Preposti e, in ultima istanza, al Titolare.

12.4.3 Tipologie di verifiche

Le verifiche di sicurezza possono essere di quattro tipi:

a) ***puntuali preventive***: attività di verifica effettuate precedentemente all'implementazione, o modifica sostanziale, di un sistema o processo per verificarne la rispondenza alle politiche di sicurezza;
b) ***puntuali a posteriori***: attività di verifica effettuate a seguito del verificarsi di incidenti di sicurezza;
c) ***periodiche*****:** attività di verifica, manuali o automatizzate, per contrastare minacce incombenti o potenziali, effettuate con cadenza periodica programmata;
d) ***a campione***: attività di verifica effettuate su campioni scelti secondo criteri prestabiliti e ad intervalli di tempo non fissi.

12.4.3.1 Verifiche puntuali preventive

Prima della messa in produzione di un sistema (hardware o software), o di modifiche sostanziali di sistemi già in produzione, devono essere effettuate le verifiche necessarie per assicurare il rispetto delle politiche di sicurezza della Provincia e, nel caso il sistema preveda il trattamento di dati personali, delle adeguate misure di sicurezza (se del caso, anche sulla base delle indicazioni contenute negli specifici provvedimenti del Garante e di Agid).

Le verifiche sono effettuate dalla Struttura competente in materia di sicurezza informatica e sono condotte seguendo il "Piano di test" preventivamente concordato fra i soggetti interessati.

Al termine delle verifiche, è redatto il "Verbale di test" (modello allegato al termine della presente Sezione II) secondo lo schema del "Piano di test".

Il sistema può essere messo in produzione solo se le verifiche hanno dato esito positivo; in caso contrario, nel "Verbale di test" sono indicati gli adeguamenti necessari.

12.4.3.2 Verifiche puntuali a posteriori

La verifica puntuale a posteriori può essere avviata a seguito di:

a) segnalazione di un soggetto terzo;
b) verifica di sicurezza, periodica o a campione.

Relativamente alle segnalazioni di cui alla lettera a):

- non sono tenute in considerazione quelle anonime;
- devono essere rivolte, per iscritto, alla Struttura competente in materia di sicurezza informatica.

Allorché si verifichi un evento di sicurezza (lettera b)), il fattore decisivo è la capacità di rispondere in modo veloce ed efficace: la rapidità con cui un'organizzazione è in grado di riconoscere un incidente, o un attacco, e successivamente analizzarlo e contrastarlo, incide sul danno, inferto o potenziale, ed abbassa i costi di ripristino.

Per questo è fondamentale che, a seguito di un "evento di sicurezza" (una violazione, o minaccia di imminente violazione, delle norme di sicurezza), il soggetto competente allo svolgimento dei controlli avvii un processo di verifica al fine di:

a) accertare se si tratta di un incidente di sicurezza;
b) adoperarsi per contenere gli effetti dannosi provocati dall'incidente, isolando il sistema o i sistemi colpiti;
c) dare disposizioni affinché siano conservati i dati necessari da mettere eventualmente a disposizione delle autorità giudiziarie;
d) adoperarsi per ripristinare il sistema o i sistemi coinvolti;
e) effettuare un'analisi delle cause dell'incidente;

f) effettuare, nell'ipotesi in cui si riscontrino elementi che inducano ad ipotizzare un utilizzo improprio degli strumenti, le ulteriori verifiche necessarie ad acquisire i dati, anche personali, strettamente necessari da comunicare ai soggetti di cui alla lettera g);

g) redigere il "Rapporto incidente di sicurezza" (modello allegato al termine della presente Sezione II). Tale rapporto è integrato dalle prove raccolte, affinché i responsabili dei sistemi coinvolti possano effettuare le ulteriori valutazioni e adottare le azioni conseguenti. Il Rapporto di incidente deve essere conservato agli atti, anche nel caso in cui i controlli siano affidati a soggetto esterno.

h) inviare, in forma riservata, il Rapporto incidente di sicurezza ai responsabili coinvolti o ad altri Titolari del trattamento di dati personali, nonché (qualora l'incidente integri una violazione dei dati) all'Ufficio Organizzazione e gestione privacy.

Relativamente ai log di navigazione è possibile, qualora sia riscontrato un incidente di sicurezza, verificare il contenuto dei siti visitati soltanto nel caso in cui le relative informazioni siano indispensabili al fine di accertare se vi sia stato un utilizzo proprio, o improprio, degli strumenti messi a disposizione dall'Amministrazione. Le ulteriori verifiche, inoltre, se necessario, possono essere effettuate sui dati relativi a più giornate lavorative, anche consecutive, con un limite massimo di 20 giornate lavorative.

Qualora, anche a seguito delle ulteriori verifiche effettuate, il soggetto competente allo svolgimento dei controlli riscontri elementi che confermino un possibile uso improprio delle strumentazioni messe a disposizione dalla Provincia, associa il nominativo dell'utilizzatore alla postazione client e successivamente procede come di seguito disciplinato:

- trasmette, al Dirigente al quale è assegnato il soggetto sottoposto al controllo, il Rapporto incidente di sicurezza affinché anch'egli possa effettuare le valutazioni di competenza, con particolare riferimento alla pertinenza (o stretta attinenza), o meno, dei dati di navigazione con l'attività lavorativa;
- contestualmente comunica, al soggetto coinvolto, la verifica in corso.

Sarà cura del Dirigente convocare il soggetto interessato per una tempestiva audizione, affinché possa fornire chiarimenti, motivazioni ed osservazioni a proposito di quanto rilevato. All'audizione possono essere presenti, su richiesta del Dirigente e/o del soggetto coinvolto, il responsabile della Struttura competente in materia di sicurezza informatica (o altro tecnico addetto alla sicurezza da questi individuato).

12.4.3.3 Verifiche periodiche

I sistemi informativi sono soggetti a verifica costante.

Tali verifiche devono essere opportunamente documentate, da parte del personale che le effettua, e la documentazione deve essere conservata agli atti, pure nel caso in cui i controlli siano affidati a soggetto esterno.

Nell'ipotesi in cui si riscontri un incidente di sicurezza, si deve procedere come anzi specificato.

I controlli devono essere effettuati, con cadenza periodica, e precedentemente pianificati. A seconda della frequenza con cui vengono svolti, si distinguono due ulteriori tipologie.

12.4.3.3.1 Verifiche periodiche effettuate con cadenza inferiore ai 15 giorni

Tali verifiche mirano al controllo della sicurezza dei trattamenti di dati personali effettuati; tutti gli utenti del Sistema informativo che gestisce i trattamenti della Provincia devono essere resi edotti di tali iniziative.

Esempi di tali attività sono:

a) verifiche giornaliere sui log del sistema firewall;
b) verifiche dei software installati sui sistemi server e client;
c) verifiche sul traffico di rete;
d) verifiche sull'efficienza dei sistemi proxy;
e) verifiche sui sistemi antivirus;
f) verifiche sull'efficacia dei filtri antispam.

12.4.3.3.2 Verifiche periodiche effettuate con cadenza superiore ai 15 giorni

Tali verifiche mirano al controllo sulla corretta applicazione e sull'efficiente funzionamento delle misure di sicurezza nell'ambito del Sistema informativo che gestisce i trattamenti della Provincia, e devono essere pianificate dal soggetto competente allo svolgimento dei controlli utilizzando il "Piano di Test" e condividendolo, preventivamente, con i soggetti interessati.

A titolo esemplificativo, rientrano in tale categoria le seguenti iniziative:

a) verifiche sull'avvenuta adozione e sul contenuto degli atti di designazione dei Responsabili del trattamento o degli Addetti;
b) verifiche sui trattamenti della Provincia e sul loro continuo aggiornamento;
c) verifiche sulla corretta applicazione delle procedure di controllo degli accessi presso le portinerie;
d) verifiche sulle configurazioni dei sistemi server e client;
e) verifiche su sviluppo, configurazione e deployment delle applicazioni informatiche;
f) verifiche sugli accessi remoti alla rete provinciale (VPN, dial-up, ecc.);
g) verifiche sugli apparati di rete e sui sistemi (vulnerability scan, penetration test, ecc.);
h) verifiche sulla corretta applicazione delle misure di sicurezza, nonché quelle consistenti nel rispetto dei comportamenti specificati nella deliberazione della Giunta provinciale n. 1037/2010.

1) Modello di verbale di test

Introduzione

Obiettivo

- L'obiettivo delle attività di test è la verifica dell'efficacia delle singole misure di continuità, tecnologiche ed organizzative che lo compongono.
- Obbiettivo secondario di tali attività è la formazione e l'addestramento del personale coinvolto, in quanto l'adeguatezza delle singole misure di continuità dipende in larga misura dalla capacità dello stesso di porre in essere, correttamente e tempestivamente, in caso di necessità, quanto predisposto.
- Lo scopo del presente documento è di descrivere tutte le attività necessarie per la corretta pianificazione, e successiva esecuzione, del test programmato per data del test relativo alla verifica *elementi da verificare*.

Perimetro

Perimetro di applicazione del test.

INFORMAZIONI GENERALI

Tipologie di verifiche

Tipologie delle verifiche da effettuare.

Responsabile dei Test

Identificazione del responsabile del test

Risorse Umane coinvolte

Individuazione puntuale delle risorse umane, interne ed esterne, coinvolte.

Asset coinvolti

Individuazione puntale degli asset coinvolti nel test.

Pianificazione dell'attività

Pianificazione dettagliata delle attività programmate.

Obiettivi delle verifiche

Descrizione degli obiettivi delle verifiche.

Risultati attesi ed elementi da verificare

Punti di criticità

Punti di criticità che hanno suggerito l'effettuazione del test.

procedure di emergenza e di rollback

Procedure di emergenza previste.

stima dei costi del test

Stima dei costi del test

Relativamente alle risorse interne è previsto un costo aziendale come nella seguente tabella:

Tipologia di costo	Quantità
Ore "Personale"	

valorizzate a costo standard con le maggiorazioni del caso per il personale vigenti (circa xxxx Euro).

2) Modello di rapporto sull'incidente di sicurezza

DENOMINAZIONE INCIDENTE

DATA INCIDENTE

INTRODUZIONE

Premessa

Gli incidenti di sicurezza possono essere seri, come una violazione che compromette le operazioni cruciali o il guasto di un apparato o il verificarsi di un evento naturale, o minori, come una mancanza di rispetto per una procedura a causa di un errore. Investire tempo e risorse nello sviluppo delle politiche e delle procedure, usando i controlli di sicurezza per le reti, le applicazioni e le operazioni di revisioni e di monitoraggio, non ci garantisce che gli incidenti non avvengano.
Una progettazione attenta della governance della Sicurezza delle Informazioni richiede anche le procedure per una risposta agli incidenti.
Le procedure per rispondere a un incidente dovrebbero chiaramente definire cosa si intende per incidente, le persone responsabili per le risposte, le persone e le strutture che occorre informare degli incidenti, i passi per minimizzare le minacce, le procedure per il ripristino e le revisioni e le analisi ex post.
Gli incidenti sono delle minacce alle organizzazioni, ma sono anche delle occasioni per valutare i limiti delle procedure e le operazioni esistenti. Occorre eseguire una revisione ex post dopo ogni incidente per capire come l'evento è avvenuto all'interno dell'infrastruttura di sicurezza esistente e si richiedono cambiamenti tali da evitare un incidente simile nel futuro.

Scopo

La gestione degli incidenti è un complesso processo che comincia dalla segnalazione di un evento, procedendo poi con la gestione e l'analisi dell'evento stesso e terminando con delle azioni di risposta e propositive.

Il presente documento ha lo scopo di illustrare i passi percorsi per analizzare l'incidente rilevato il giorno **.**.****, riportando anche le conclusioni del lavoro svolto.

scenario di analisi

scenario dell'incidente di sicurezza

Descrizione dello scenario dell'incidente (Rete, desktop, ambiente).

descrizione dell'incidente di sicurezza

Descrizione cronologica degli eventi e di eventuali misure intraprese

Evidenze

Elencazione delle evidenze raccolte (log, configurazioni, testimonianze).

Passi dell'indagine effettuata

*Descrizione delle attività di indagine svolte***.**

Cause dell'Incidente

Descrizione delle cause che hanno generato l'incidente se individuate.

Conclusioni

Conclusioni sull'accaduto.

Azioni correttive

Descrizione delle azioni correttive intraprese o da intraprendere individuate durante la fase di gestione dell'incidente.

ELENCO ESEMPLIFICATIVO DI CASISTICHE CHE POTREBBERO CONFIGURARE UN *DATA BREACH*

TRATTAMENTI ELETTRONICI

Eventi accidentali

determinati da casi fortuiti, o comportamenti involontari, che causano la perdita delle caratteristiche di sicurezza dei dati (riservatezza, integrità, disponibilità):

- **esecuzione erronea di comandi e/o procedure:** ad esempio, formattazione di dispositivi di memorizzazione;

- **rottura delle componenti *hardware*:** ad esempio, distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura o di elettricità, ovvero per umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, allagamenti, ecc.;

- **malfunzionamento del *software*:** ad esempio, esecuzione di uno *script* automatico non autorizzato, o errori di programmazione che causano *output* errati, ecc.;

- **comunicazione (e diffusione) di dati a persona diversa dall'interessato**, ad esempio in evasione di reclami/richieste di informazioni avanzate da persone diverse dall'interessato, o per errata pubblicazione delle informazioni personali su portali *web*;

- **guasti alla rete aziendale**: ad esempio, interruzione delle comunicazioni durante il trasferimento dei dati e perdita dei dati durante la trasmissione, ecc.

Eventi dolosi

realizzati intenzionalmente dal personale interno, o da soggetti esterni, e realizzati tramite:

1. **accesso non autorizzato ai dati**, sfruttando vulnerabilità dei sistemi interni e delle reti di comunicazione;

2. **compromissione o rilevazione abusiva di credenziali** di autenticazione;

3. **utilizzo di *software* specificatamente orientato alla compromissione dell'integrità** applicativa del *device*.

TRATTAMENTI NON ELETTRONICI

Eventi accidentali

determinati da casi fortuiti, o comportamenti involontari, che causano la perdita delle caratteristiche di sicurezza dei dati (confidenzialità, integrità, disponibilità):

- **distruzione di documenti contenenti dati personali**, ad esempio a seguito di incendio, allagamento, o altri eventi fortuiti;

- **smarrimento di documenti contenenti dati personali**;
- **comunicazione involontaria di dati a persona diversa dall'interessato**, ad esempio in evasione di reclami/richieste di informazioni avanzate da persone diverse dall'interessato.

Eventi dolosi

realizzati intenzionalmente dal personale interno, o da soggetti esterni, quali:

- **distruzione dei documenti** contenenti dati personali;
- **accesso non autorizzato** ai documenti, ad archivi, ecc., contenenti dati personali;
- **sottrazione (furto) di documenti/supporti** contenenti dati personali.

SEZIONE III

MODULISTICA

N.B. La modulistica allegata alla presente deliberazione costituisce lo schema-tipo base conforme alla vigente normativa. Non essendo concepibile la predisposizione, da parte dell'Ufficio Organizzazione e gestione della privacy, di un modello specifico e definitivo per ogni articolazione organizzativa della Provincia, ciascun modello (che reca un codice identificativo e la relativa data di aggiornamento) potrà/dovrà essere opportunamente adattato da parte di ciascuna Struttura, previa autorizzazione del Dirigente e avvalendosi del Referente privacy, ferme restando le inderogabili prescrizioni normative; ciò, tenendo altresì presenti le prescrizioni contenute nelle Regole deontologiche e nelle Autorizzazioni del Garante.
Con l'occasione, si rammenta che ogni Struttura provinciale è tenuta a predisporre un modello di informativa generale, da pubblicare sul sito istituzionale della Provincia.
I modelli sono comprensivi di note di chiarimento per la compilazione (ovviamente, da eliminare nel modulo definitivamente adottato dalla Struttura), evidenziate in giallo.

Mod. (I.) - copia per l'Amministrazione
Ed. 1-2019

INFORMATIVA
EX ARTT. 13 E 14 DEL REGOLAMENTO UE n. 679 del 2016

Il Regolamento Europeo UE/2016/679 (di seguito il "Regolamento") stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
In osservanza del principio di trasparenza previsto dagli artt. 5 e 12 del Regolamento, la Provincia autonoma di Trento Le fornisce le informazioni richieste dagli artt. 13 e 14 del Regolamento (rispettivamente, raccolta dati presso l'Interessato e presso terzi).

Titolare del trattamento dei dati personali è la Provincia autonoma di Trento (di seguito, il "Titolare"), nella persona del legale rappresentante (Presidente della Giunta Provinciale in carica), Piazza Dante n. 15, 38122 – Trento, tel. 0461.494697, *fax* 0461.494603 *e-mail* direzionegenerale@provincia.tn.it, pec segret.generale@pec.provincia.tn.it.

Preposto al trattamento è il Dirigente *pro tempore* del *[indicare lo specifico Dipartimento/Servizio/Umse/Umst/Agenzia/ecc.]*……..; i dati di contatto sono: indirizzo ……., tel. ……., *fax* ……., *e-mail* …… . Il Preposto è anche il **soggetto designato per il riscontro** all'Interessato in caso di esercizio dei diritti *ex* artt. 15 – 22 del Regolamento, di seguito descritti.

I dati di contatto del **Responsabile della protezione dei dati** (RPD) sono: via Mantova n. 67, 38122 – Trento, *fax* 0461.499277, *e-mail* idprivacy@provincia.tn.it (indicare, nell'oggetto: "Richiesta intervento RPD *ex* art. 38 Reg. UE").

[FRASE DA INSERIRE SOLO NELL'INFORMATIVA AI DIPENDENTI] L'elenco degli amministratori di sistema, la cui attività riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, è consultabile presso la specifica struttura a cui è assegnato il dipendente. L'elenco di tali amministratori di sistema, nominati da Trentino Digitale S.p.a. quale Responsabile del trattamento, è consultabile presso la *intranet* provinciale.

Il trattamento dei Suoi dati personali sarà improntato al rispetto della normativa sulla protezione dei dati personali e, in particolare, ai principi di correttezza, liceità e trasparenza, di limitazione della conservazione, nonché di minimizzazione dei dati in conformità agli artt. 5 e 25 del Regolamento.

1. FONTE DEI DATI PERSONALI
I Suoi dati
[INSERIRE IL FLAG E COMPILARE]
☐ sono stati raccolti presso ……
☐ provengono dalle seguenti fonti accessibili al pubblico: ……
☐ sono stati raccolti presso l'Interessato (Lei medesimo).

2. CATEGORIA DI DATI PERSONALI (INFORMAZIONE FORNITA SOLO SE I DATI SONO RACCOLTI PRESSO TERZI)
I dati personali trattati appartengono alla/e seguente/i categoria/e:
[INSERIRE IL FLAG]
☐ Dati personali diversi da particolari categorie di dati (c.d. dati comuni) –…….. *[specificare tipologia]*
☐ Dati personali appartenenti a particolari categorie di dati (c.d. dati sensibili) –…….. *[specificare*

tipologia]

- ☐ Dati personali relativi a condanne penali e ai reati o a connesse misure di sicurezza (c.d. dati giudiziari) – …… *[specificare tipologia]*
- ☐ Dati relativi allo stato di salute, genetici, biometrici

3. FINALITA' DEL TRATTAMENTO

Il principio di minimizzazione prevede come possano essere raccolti e trattati soltanto i dati personali pertinenti e non eccedenti alle specifiche finalità del trattamento.
Il principio di limitazione della conservazione consiste nel mantenere i dati in una forma che consente l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità, salvo casi eccezionali.
Anche per tali ragioni, nonché nel rispetto degli artt. 13 e 14 del Regolamento, di seguito Le indichiamo specificamente la **finalità del trattamento** e la **base giuridica** che consente il trattamento dei Suoi dati:

per l'**esecuzione di un compito di interesse pubblico / connesso all'esercizio di pubblici poteri** di cui è investito il Titolare (art. 6.1, lett. e), del Regolamento) e, in particolare, per *[inserire la specifica finalità e la norma su cui si fonda il trattamento]* ……, ai sensi e per gli effetti di ……..

[ALTERNATIVE]

[A. Qualora il conferimento fosse obbligatorio e le conseguenze fossero le seguenti] Il conferimento dei Suoi dati personali è obbligatorio per le finalità di cui sopra e per tutte quelle ausiliarie e connesse (quali, ad esempio, attività di controllo e consultive), *[ALTERNATIVE]* in quanto obbligo legale *[OPPURE]* in quanto obbligo contrattuale *[OPPURE]* in quanto requisito necessario per la conclusione del contratto; il rifiuto al conferimento dei dati comporterà l'impossibilità di *[ALTERNATIVE (ESEMPI)]* fornire la prestazione/corrispondere alla richiesta connessa alla specifica finalità/concludere il contratto.

[B. Qualora il conferimento fosse facoltativo e le conseguenze fossero le seguenti] Il conferimento dei Suoi dati personali è facoltativo; il rifiuto al conferimento dei dati, però, comporterà l'impossibilità di *[ALTERNATIVE (ESEMPI)]* fornire la prestazione/corrispondere alla richiesta connessa alla specifica finalità/concludere il contratto.

[OPZIONE, da inserire solo se sussistono dati sensibili / giudiziari]
Con riferimento ai dati personali riconducibili a "categorie particolari", *ex* art. 9 del Regolamento (quali, ad esempio, quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, ovvero ancora quelli relativi alla salute, o alla vita sessuale, o all'orientamento sessuale)/relativi a condanne penali, o a reati, o a connesse misure di sicurezza *ex* art. 10 del Regolamento, si precisa altresì come il relativo trattamento sia necessario, ai sensi dello stesso art. 9.2, lett. g), del Regolamento, per un **motivo di interesse pubblico rilevante** *[descrivere la finalità]* (……), in particolare così come individuato *[ALTERNATIVE]* dalla Legge ……/dall'art. 2-*sexies*, comma 2, lett. …..), del D. Lgs. 196/03.

Per massima chiarezza, Le precisiamo che, essendo fondato sulle predette basi, non è quindi necessario il Suo consenso al trattamento di tali dati personali.

[OPZIONE, da inserire solo se sussistono dati relativi allo stato di salute / biometrici / genetici]
Quanto ai dati relativi allo stato di salute/biometrici/genetici, che non possono in ogni caso essere diffusi, si evidenzia altresì come tali dati siano trattati in conformità all'art. 2-*septies* del D. Lgs. 196/03

e, in particolare, nel rispetto di quanto specificamente previsto dal Garante. *[OPZIONE, da inserire solo qualora un eventuale provvedimento del Garante richiedesse il consenso per il trattamento dei dati genetici. In tal caso,* ***aggiungere lo specifico consenso in calce al modulo****]* Per i dati genetici, inoltre, è necessario il Suo consenso esplicito.

4. MODALITA' DEL TRATTAMENTO

Il trattamento sarà effettuato *[ALTERNATIVE]* con modalità cartacee/con modalità cartacee e con strumenti automatizzati (informatici/elettronici) con logiche atte a garantire la riservatezza, l'integrità e la disponibilità dei dati stessi / con strumenti automatizzati (informatici/elettronici) con logiche atte a garantire la riservatezza, l'integrità e la disponibilità dei dati stessi.

I Suoi dati saranno trattati, esclusivamente per le finalità di cui sopra, dal personale dipendente debitamente istruito e, in particolare, da Preposti al trattamento (Dirigenti), appositamente nominati, nonché da Addetti al trattamento dei dati, specificamente autorizzati.

Sempre per le finalità indicate, i Suoi dati potranno essere trattati da soggetti che svolgono attività strumentali (*[inserire per macro-categorie; ad esempio: fornitori di servizi informatici]* quali……..) per il Titolare, che prestano adeguate garanzie circa la protezione dei dati personali e nominati **Responsabili del trattamento** *ex* art. 28 del Regolamento. L'elenco aggiornato dei Responsabili è consultabile *[OPZIONI]* sul sito ……/presso i nostri uffici siti in …….

5. PROCESSI DECISIONALI AUTOMATIZZATI E PROFILAZIONE

[ALTERNATIVE; si propongono alcune soluzioni, ciascuna da adattare al caso di specie. Il trattamento sub D. è consentito solo se la decisione ***è necessaria*** *per la conclusione o l'esecuzione di un contratto tra l'Interessato e il Titolare, oppure se la decisione* ***è prevista da una norma*** *che precisa le misure adeguate a tutela dei diritti dell'Interessato; inoltre, salvo casi eccezionali, tali decisioni non si basano su "categorie particolari" di dati]*

[A. Se non c'è profilazione] E' esclusa l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

[B. Per la "profilazione generica"] Il trattamento è eseguito anche mediante una profilazione generale, cioè eseguita con strumenti non automatizzati: *[specificare in che termini viene effettuata]*

[C. Per le "decisioni basate sulla profilazione"] Il trattamento è eseguito anche mediante un processo decisionale automatizzato *[EVENTUALE]*, compresa la profilazione; in particolare, tale trattamento automatizzato dei dati, consiste nell'utilizzo dei dati personali per valutare, ad esempio: il rendimento professionale, la situazione economica, la salute, le preferenze, l'affidabilità, il comportamento o l'ubicazione. La logica utilizzata è la seguente: *[indicare in modo semplice e conciso la metodologia di elaborazione dei dati / il funzionamento dello specifico software]* ……; pertanto, le conseguenze di tale specifico trattamento sono le seguenti: *[indicare l'effetto del trattamento automatizzato o della profilazione]* ……

[D. Per le "decisioni totalmente automatizzate"] Il trattamento è eseguito mediante un processo decisionale interamente automatizzato *[EVENTUALE]*, compresa la profilazione; in particolare, tale trattamento automatizzato dei dati, consiste nell'utilizzo dei dati personali per valutare, ad esempio: il rendimento professionale, la situazione economica, la salute, le preferenze, l'affidabilità, il comportamento o l'ubicazione. La logica utilizzata è la seguente: *[indicare in modo semplice e conciso la metodologia di elaborazione dei dati / il funzionamento dello specifico software]* ……; pertanto, le conseguenze di tale specifico trattamento sono le seguenti: *[indicare l'effetto del trattamento automatizzato o della profilazione]* ……

6. COMUNICAZIONE E DIFFUSIONE DEI DATI (CATEGORIE DI DESTINATARI)

[ALTERNATIVE]

I Suoi dati non saranno comunicati.

[OPPURE]

La informiamo che i Suoi dati saranno comunicati alle seguenti categorie di destinatari:

- ……;
- ……

[ALTERNATIVE] per l'adempimento di un obbligo legale *[OPPURE]* per l'adempimento di un obbligo contrattuale *[OPPURE]* in quanto requisito necessario per la conclusione del contratto.

I Suoi dati personali *[ALTERNATIVE]* non saranno diffusi *[OPPURE]* , fermo il divieto di diffusione dei dati relativi alla salute (oltre che di quelli genetici e biometrici), saranno diffusi ai sensi e per gli effetti delle seguente norma: ……

7. TRASFERIMENTO *EXTRA* UE

[ALTERNATIVE]

I dati personali non saranno trasferiti fuori dall'Unione Europea.

[OPPURE]

I dati personali saranno trasferiti fuori dall'Unione Europea e, in particolare, in *[indicare il/i Paese/i]* …… Il trasferimento dei dati nel/i Paese/i terzo/i indicato/i è tutelato da: *[specificare quale delle condizioni previste agli artt. 44 e ss. del Regolamento UE 2016/679 consentono il trasferimento extra U.E. e i mezzi per ottenere una copia dei dati o il luogo dove sono stati resi disponibili]* ……

8. PERIODO DI CONSERVAZIONE DEI DATI

[Indicare precisamente i termini]

In osservanza del succitato principio di limitazione della conservazione, Le comunichiamo che il periodo di conservazione dei Suoi dati personali *[OPZIONALE]*, come previsto nel "massimario di scarto" / *[EVENTUALE, se esistono eventuali norme di legge]* da... ……, è di:

- …… per i dati diversi da quelli compresi nelle "particolari categorie",
- …… per i dati appartenenti alle "categorie particolari",

A) …… per i dati relativi alle condanne penali/reati,

dalla raccolta dei dati stessi.

Trascorso tale termine i dati saranno cancellati *[OPZIONE, se si realizza tale eventualità e non è già stata prevista tra le finalità del trattamento]*, fatta salva la facoltà del Titolare di conservarli ulteriormente per trattarli a fini di archiviazione nel pubblico interesse, di ricerca scientifica, o storica, o a fini statistici.

[OPZIONE, se prevista l'opzione B., C. o D. al § 5. dell'informativa] Relativamente ai dati trattati per finalità di profilazione, o mediante processi decisionali automatizzati, il termine di conservazione è di ……

9. DIRITTI DELL'INTERESSATO

Lei potrà esercitare, nei confronti del Titolare ed in ogni momento, i diritti previsti dal Regolamento.
In base a tale normativa Lei potrà:

- chiedere l'accesso ai Suoi dati personali e ottenere copia degli stessi (**art. 15**);
- qualora li ritenga inesatti o incompleti, richiederne, rispettivamente, la rettifica o l'integrazione (**art. 16**);
- se ricorrono i presupposti normativi, richiederne la cancellazione (**art. 17**), o esercitare il diritto di limitazione (**art. 18**);

- opporsi al trattamento dei Suoi dati (compresa l'eventuale profilazione) in qualsiasi momento, per motivi connessi alla Sua situazione particolare (**art. 21**).
- *[OPZIONE. Se prevista l'opzione D. al § 5. dell'informativa e tale opzione è necessaria per la conclusione o esecuzione del contratto]* in relazione alla decisione totalmente automatizzata, ottenere l'intervento umano da parte del Titolare, esprimere la propria opinione e contestare la decisione (**art. 22**).

Ai sensi dell'**art. 19**, nei limiti in cui ciò non si riveli impossibile o implichi uno sforzo sproporzionato, il Titolare comunica a ciascuno degli eventuali destinatari cui sono stati trasmessi i dati personali le rettifiche, o cancellazioni, o limitazioni del trattamento effettuate; qualora Lei lo richieda, il Titolare Le comunicherà tali destinatari.

In ogni momento, inoltre, Lei ha diritto di proporre reclamo al Garante per la protezione dei dati personali.

[OPZIONE, solo se prestato il consenso per i dati genetici (ai sensi di un eventuale provvedimento in tal senso da parte del Garante)]

Con riferimento al consenso rilasciato per i dati genetici, Lei ha altresì il diritto di revocare il consenso stesso in qualsiasi momento e gratuitamente, senza pregiudicare la liceità del trattamento sino al momento della revoca, mediante comunicazione a …… o inviando una *e-mail* a ……..

Dichiaro di aver ricevuto e preso visione della presente informativa

data e firma _____

Mod. (D.1)
Ed. 1-2019

Alla Provincia autonoma di Trento – P.zza Dante, 15 – 38122 – Trento – Titolare del trattamento (c.a. Direttore generale)

Al Dirigente pro tempore del…../*indicare Dipartimento, Servizio, Unità di missione, Agenzia]* – Preposto al trattamento

OGGETTO: **ESERCIZIO DEI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

Il/La sottoscritto/a_____

nato/a a_____ il _____

☐ in qualità di interessato

[in caso di interessato deceduto]
☐ in quanto avente un interesse proprio / a tutela dell'interessato, in qualità di mandatario / per ragioni familiari meritevoli di protezione (art. 2-*terdecies* D. Lgs. 196/03):
(*specificare e documentare l'interesse proprio / la tutela dell'interessato e il mandato conferito / le ragioni familiari meritevoli di protezione*)
_____
_____
_____

(BARRARE SOLO LE CASELLE CHE INTERESSANO)

Accesso ai dati personali (art. 15 del Regolamento UE 2016/679)

Il/la sottoscritto/a **chiede**

ai sensi dell'art. 15 del Regolamento UE 2016/679 di confermargli/le se sia in corso un trattamento di dati personali che lo/la riguardano e, qualora la conferma dia esito positivo, di fornirgli/le una copia dei dati stessi.

La presente richiesta riguarda (*al fine di fornire un più celere riscontro, indicare, se possibile, i dati personali, le categorie di dati personali o il trattamento cui si fa riferimento*):

_____

_____

Richiesta di conoscere alcune notizie sul trattamento (art. 15 del Regolamento UE 2016/679)

Il/la sottoscritto/a **chiede** di conoscere:

- ☐ le finalità del trattamento dei dati che lo riguardano;
- ☐ le categorie di dati personali trattati;
- ☐ i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare in caso di trasferimento dei dati in Paesi terzi o ad organizzazioni internazionali;
- ☐ il periodo di conservazione dei dati ovvero il criterio utilizzato per determinare tale periodo;
- ☐ l'esistenza di un processo decisionale automatizzato, la logica utilizzata, l'importanza e le conseguenze che il trattamento hanno per l'interessato;
- ☐ l'origine dei dati, se raccolti presso terzi;
- ☐ le adeguate garanzie, applicate ai sensi dell'art. 46 del Regolamento UE 2016/679, se i dati personali sono trasferiti ad un Paese terzo (fuori dall'Unione Europea) o ad un'organizzazione internazionale.

La presente richiesta riguarda *(indicare, se possibile, i dati personali, le categorie di dati o il trattamento cui si fa riferimento)*:

_____

_____

Richiesta di intervento sui dati (rettifica, integrazione, cancellazione e limitazione – artt. 16, 17, 18 e 19 del Regolamento UE 2016/679)

Il/la sottoscritto/a **richiede**:

- ☐ la **correzione** del/dei seguente/i dato/i personale/i *(indicare quale/i dato/i personale/i)* perché errato/i, nella forma seguente:

  _____;

- ☐ l'**integrazione** del/dei seguente/i dato/i personale/i (*indicare quale/i dato/i personale/i)* perché incompleto/i, nella forma seguente:

  _____;

- ☐ la **cancellazione**[2] del/dei seguente/i dato/i personale: (*indicare quale/i dato/i personale/i)*

  _____
  per i motivi seguenti: (*barrare laddove necessario*)

  - ☐ perché la finalità istituzionale della Provincia è stata raggiunta

[2] La cancellazione del dato non si applica 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 previsto dal diritto europeo o dello Stato membro cui è soggetto il titolare del trattamento; c) per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio dei pubblici poteri; d) per motivi di interesse pubblico nel settore della sanità pubblica; e) ai fini di archiviazione nel pubblico interesse, di ricerca scientifica e storica o a fini statistici; f) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Deroghe possono essere altresì previste in base agli ordinamenti giuridici nazionali.

- ☐ perché è stata fatta opposizione dal/dalla sottoscritto/a ed ha avuto esito a lui/a lei favorevole
- ☐ perché il dato o i dati sono stati trattati in violazione di legge
- ☐ per adempiere al seguente obbligo legale (*indicarlo in breve)*……..
- ☐ *[OPZIONALE: da inserire soltanto qualora l'informativa preveda il consenso e, quindi, la revoca del consenso tra i diritti dell'interessato]* per revoca del consenso

_____

_____

☐ la **limitazione del trattamento**[3] per il/i dato/i seguente/i: (*indicare quale/i dato/i personale/i)*

_____

per i seguenti motivi (barrare laddove necessario):

- ☐ perché si ritiene che il dato o i dati non siano esatti e fino al momento in cui verranno rettificati
- ☐ perché, pur ritenendo il trattamento dei dati illecito, il/la sottoscritto/a è contrario alla cancellazione dei dati
- ☐ perché i dati, pur non essendo più necessari alla Provincia, servono al/alla sottoscritto/a per l'accertamento, l'esercizio o la difesa di un proprio diritto in sede giudiziaria
- ☐ il/la sottoscritto/a si è opposto al trattamento dei propri dati ed è in attesa della verifica in merito alla prevalenza dei suoi legittimi motivi

☐ di **conoscere** i destinatari (a cui sono stati trasmessi i dati personali) a cui il Titolare ha comunicato le rettifiche/cancellazioni/limitazioni

Opposizione al trattamento (art. 21 del Regolamento UE 2016/679)

Il/la sottoscritto/a **si oppone** al trattamento del/dei seguente/i dato/i personale:
(*indicare quale/i dato/i personale/i)*

_____

per i seguenti motivi connessi alla situazione particolare (*indicarli in breve*):

_____

_____

_____

[OPZIONALE: la seguente sezione ("Diritti connessi ad una decisione esclusivamente basata su un trattamento automatizzato") dev'essere inserita solo qualora la specifica informativa contempli tali diritti dell'interessato]

Diritti connessi ad una decisione esclusivamente basata su un trattamento automatizzato, compresa la profilazione (art. 22 del Regolamento UE 2016/679)

Il/la sottoscritto/a, relativamente alla decisione derivante dal

[3] Significa che, ad esclusione della conservazione, ogni operazione di trattamento del dato oggetto di limitazione è temporaneamente sospeso. I dati potranno essere trattati dalla Provincia solo: a) per l'esercizio o la difesa giudiziale di un diritto da parte della Provincia, b) per la tutela dei diritti di un terzo, oppure c) per motivi di rilevante interesse pubblico.

trattamento esclusivamente automatizzato:

- ☐ esercita il diritto di ottenere un intervento decisionale umano;
- ☐ esprime la propria seguente opinione:_____
- ☐ contesta la decisione assunta

Il/la sottoscritto/a si riserva il diritto di ricorrere all'Autorità giudiziaria, o di proporre reclamo al Garante per la protezione dei dati personali se entro 1 mese (estensibile fino a tre mesi in caso di particolare complessità) dal ricevimento della presente istanza non perverrà un riscontro idoneo.

Recapito per le comunicazioni:

Indirizzo di posta elettronica:

_____

oppure

Indirizzo postale:

Via/Piazza_____

Comune_____

Provincia _____ Codice postale _____

oppure

telefax:_____

oppure

telefono:_____

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____

_____

_____

Allegare copia di un documento di riconoscimento:

_____

_____

_____ _____

Luogo e data *Firma*

Mod. (A.C.1)
Ed. 1-2018

RICHIESTA DEL CONTENUTO
DEL CONTRATTO DI CONTITOLARITA'

Alla Provincia autonoma di Trento

e, p.c., al Responsabile della protezione dei dati personali (RPD)

Oggetto: richiesta del contenuto del contratto di contitolarità

Il/La sottoscritto/a ……., in qualità di interessato (al quale si riferiscono i dati) richiede, ai sensi dell'art. 26 del Reg. UE 2016/679, di accedere al contenuto essenziale del contratto di contitolarità dei trattamenti dei dati, stipulato tra il Vostro Ente e ……..

Resto in attesa di un cortese riscontro al seguente recapito:

……..

Cordiali saluti.

Data……..

Firma……..

Mod. (R.A.1)
Ed. 1-2019

Al/Alla Sig./Sig.ra …….

RISCONTRO AL DIRITTO DI ACCESSO
***EX* ART. 15 GDPR**

Oggetto: riscontro alla richiesta di accesso ai dati personali *ex* art. 15 GDPR

Il Dipartimento.....…… e le Strutture che allo stesso fanno capo, con riferimento alla richiesta inoltrata dal Sig. ……... ……....., hanno effettuato i seguenti trattamenti:

Trattamento 1

- i dati sono trattati per la seguente **finalità**:……..……..

- le **categorie di dati trattati riguardano**: *[specificare tipologia dati (**"dati comuni" -** (nome, cognome, indirizzo, codice fiscale, telefono, dati relativi all'ubicazione di persone ecc.); **"sensibili"** (relativi alla salute/genetici/biometrici//relativi all'origine razziale o etnica/relativi alle opinioni politiche, alle convinzioni religiose o filosofiche/relativi all'appartenenza sindacale/ relativi alla vita sessuale o all'orientamento sessuale; **"giudiziari"** (relativi a condanne penali e reati o misure di sicurezza)]*.....
……..

-*[eventuale]* i dati sono stati/saranno **comunicati alle seguenti categorie di destinatari**:
……
……..... *[eventuale, se il trasferimento è extra UE]* ai sensi delle seguenti **garanzie adeguate**: ……..

- i suoi dati sono **conservati per** *[indicare il periodo di conservazione]*: ..... ……sulla base di *[indicare la specifica legge, o regolamento, o atto organizzativo interno, o massimario di conservazione]*……

- *[da compilare solo se i dati sono raccolti presso terzi]* i suoi dati sono stati **raccolti presso** ……..……

- *[eventuale]* il trattamento comporta un processo decisionale automatizzato (compresa la profilazione) basato sulla seguente **logica**:..……... ……..…….. ……..... ……..…. e comporta, per l'interessato, le seguenti **conseguenze**…… ……..

- lei ha il diritto di chiedere, al Titolare, la rettifica o la cancellazione dei dati, nonché la limitazione del trattamento dei dati personali, o di opporsi al loro trattamento;

- ha diritto a proporre reclamo al Garante della protezione dei dati personali.

Trattamento 2

……...

Trattamento 3

……

Cordiali saluti.

Data……

Firma…….

Mod. (R.C.1)
Ed. 1-2018

Al/Alla Sig./Sig.ra …….

RISCONTRO ALLA RICHIESTA DI ACCESSO

AL CONTENUTO DEL CONTRATTO DI CONTITOLARITÀ

Oggetto: riscontro alla richiesta di accesso al contenuto del contratto di contitolarità

In riferimento alla Sua richiesta di accesso al contenuto del contratto di contitolarità presentata ai sensi dell'art. 26 del Reg. UE 2016/679, si riporta quanto segue:

- Finalità del contratto di contitolarità:……..

- Ruoli e responsabilità:……..

- Descrizione del flusso dei dati:……..

- Informativa privacy e modalità di esercizio dei diritti sui dati:……..

- Punto di contatto per l'esercizio dei diritti sui dati:……..

- Si riporta il *link* del sito *web* dove sono pubblicati *on lin*e i sopra citati contenuti essenziali del contratto: ……..

Cordiali saluti.

Data……

Firma…….

Mod. (C. 1)
Ed. 1-2018

CONTRATTO DI CONTITOLARITA'
ex art. 26 del Regolamento UE 2016/679

tra

PAT…

e

….

di seguito, congiuntamente, le "Parti"

Premesso che:

- in data …….. le Parti hanno stipulato il contratto / la convenzione avente ad oggetto ……; in forza di tale contratto / convenzione, *[descrivere le prestazioni contrattuali svolte dalle parti]*
  ……
  …….;
- per l'esecuzione del contratto / della convenzione, le Parti provvedono, in qualità di "*Co-Titolari del trattamento*" ai sensi dell'art. 26 del Regolamento UE 2016/679, al connesso trattamento dei dati personali *[descrivere, in termini generali, il trattamento dei dati: tipologia di dati, categoria degli interessati, operazioni di trattamento, eventuali destinatari di comunicazioni, profilazioni, ecc….]*…….....;
- in particolare, le Parti hanno congiuntamente determinato:
  - la/e seguente/i finalità del trattamento …….
    e
  - il/i seguente/i mezzo/i del trattamento: ……..

Tutto ciò premesso e considerato,
che costituisce parte integrante e sostanziale del presente contratto
(di seguito, il "Contratto"),
si stipula quanto segue:

Art. 1 – RIPARTIZIONE DEI RUOLI E DEI COMPITI

In relazione alle specifica natura del rapporto derivante dal contratto / dalla convenzione, alle rispettive prestazioni, e fermo il diritto dell'interessato di esercitare i suoi diritti nei confronti di ciascun Titolare, ai sensi e per gli effetti dell'art. 26 del Regolamento UE 2016/679 si conviene la seguente ripartizione di ruoli, compiti e connesse responsabilità.

[specificare le seguenti voci, ripartendo compiti e ruoli in relazione alle attività derivanti dal contratto/convenzione in essere tra le parti, se del caso anche scindendo lo stesso compito – tra i due contitolari – in relazione ai diversi trattamenti]

A. Consegna dell'informativa *ex* artt. 13 e 14 del Regolamento UE 2016/679 (nei termini di legge) e del contenuto essenziale del presente Contratto all'interessato: *[nel disciplinare il presente paragrafo, ricordarsi di precisare che l'informativa deve menzionare l'esistenza del contratto di contitolarità e il diritto dell'interessato di accedere al contenuto essenziale dello stesso]*

B. (Raccolta del consenso) *[EVENTUALE]*:

C. Riscontro ai diritti dell'interessato (punto di contatto) nei termini di legge

- accesso:
- rettifica e integrazione:
- cancellazione:
- opposizione:
- limitazione:
- eventuali ulteriori

D. Ripartizione delle specifiche operazioni del trattamento

- Raccolta, ……, …..
- ecc.
- ecc.

E. Trasferimento dei dati *extra* UE:

F. Nominativi dei DPO, "referenti" del presente Contratto e obblighi di collaborazione reciproca:

G. Rapporti con l'Autorità di Controllo e obblighi di comunicazione reciproca di eventuali ispezioni e/o contestazioni:

H. Registro dei trattamenti:

I. Adozione di misure di sicurezza idonee

- tecniche:
- organizzative:

J. Valutazione dei rischi, valutazione di impatto e consultazione preventiva dell'Autorità di controllo:

K. Gestione degli strumenti informatici e adempimenti relativi agli Amministratori di Sistema:

L. Gestione del sito *web* condiviso / della *app* condivisa, relativa *privacy policy* e gestione degli adempimenti in materia di *cookies*:

M. Segnalazione dei *data breach* all'Autorità di controllo e agli interessati nei termini di legge:

- violazione relativa a .....:
- violazione relativa a …….:
- ecc.:

N. *Altro... [ad esempio, nomina di Responsabili del trattamento, individuazione stabilimento principale, ecc.]*

ART. 2 – RESPONSABILITA'

Alla ripartizione dei compiti e ruoli di cui al presente Contratto, consegue ogni relativa assunzione di responsabilità in via esclusiva per violazioni o inadempimenti contrattuali e/o normativi, purché il danno provocato, o la violazione commessa, sia esclusiva conseguenza del comportamento, anche omissivo, della Parte stessa. Pertanto, fermo il disposto di cui all'art. 82 del Regolamento UE 2016/679, ciascuna della Parti manleva integralmente l'altra, per ogni risarcimento del danno dalla stessa provocato, ovvero per ogni applicazione di sanzioni amministrative derivante da una sua violazione normativa.

In forza di quanto previsto al paragrafo 3, dell'art. 26, del Regolamento UE 2016/679, le Parti si impegnano a tenersi costantemente informate e a collaborare tra loro, corrispondendo tempestivamente alle richieste dell'interessato anche in deroga a quanto previsto dal presente Contratto.

ART. 3 . DURATA

Il presente Contratto ha durata di ……. Le Parti si impegnano a pubblicare il contenuto del Contratto stesso, in forma sintetica, sui propri siti istituzionali.

Firme….

Mod. (R.1)
Ed. 2-2018

CONTRATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO E CONFERIMENTO DELLE RELATIVE ISTRUZIONI

Tra

Provincia autonoma di Trento, ……..

e

……., *[da valutare]* con sede legale in ……..., P. IVA …… / nato a ……., C.F……,

di seguito, congiuntamente, le "Parti".

Premesso che:

- tra la **Provincia autonoma di Trento** e la/il **…….** intercorre un rapporto di ……..., in forza del/della contratto/convenzione sottoscritto/a tra le Parti in data ……...;
- tale rapporto contrattuale implica, necessariamente, il trattamento, da parte della/del **……..**, di dati personali di cui la **Provincia autonoma di Trento** è Titolare del trattamento;
- il Regolamento UE 2016/679 (di seguito, il Regolamento) "*si applica al trattamento dei dati personali effettuato nell'ambito delle attività (…) di un Responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*";
- ai sensi dell'art. 28, paragrafo 1, del Regolamento, "*Qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato*";
- ai sensi dell'art. 29 del Regolamento, "*Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare…*";

- ai sensi dell'art. 28, paragrafo 3, del Regolamento, inoltre, "*I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico, che vincoli il Responsabile del trattamento al Titolare e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento*";
- ai sensi dell'art. 31 del Regolamento, "*…il Responsabile del trattamento... coopera…, su richiesta, con l'Autorità di controllo…*";
- ai sensi dell'art. 82, paragrafo 2, del Regolamento, il *"Responsabile del trattamento risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai Responsabili del trattamento o ha agito in modo difforme, o contrario, rispetto alle istruzioni impartite dal Titolare del trattamento*";
- a seguito delle garanzie offerte e delle dichiarazioni rilasciate dalla/dal **…… ……**, in forza di quanto previsto al considerando n. 81 del Regolamento, tale soggetto è stato ritenuto idoneo ad assumere la qualifica di Responsabile del trattamento;

Tutto ciò premesso e considerato,
che costituisce parte integrante e sostanziale del presente atto,
si conviene quanto segue.

Art. 1 - Ai sensi e per gli effetti dell'art. 28 del Regolamento, con il presente contratto (di seguito, il "Contratto") la **Provincia autonoma di Trento**, in qualità di "*Titolare del trattamento*" (di seguito, il "Titolare"), nomina **……** "*Responsabile del trattamento*" (di seguito, il "Responsabile"). Il Responsabile, pertanto, si impegna al rigoroso rispetto – con la diligenza di cui all'art. 1176, comma 2, del Codice Civile – della predetta normativa comunitaria, della relativa disciplina nazionale, nonché delle prescrizioni dell'Autorità di controllo. Ferma ogni ulteriore responsabilità nei confronti del Titolare, resta inteso che ogni forma di determinazione delle finalità e/o dei mezzi del trattamento da parte del Responsabile comporta l'assunzione, da parte dello stesso, della qualifica di Titolare del trattamento, con ogni ulteriore conseguenza.

Art. 2 - I dati personali trattati dal Responsabile concernono *[vedi le definizioni di cui all'art. 4, nn. 13), 14), 15) e art. 9 del Regolamento]* ……
……..; le categorie di interessati coinvolti nel trattamento riguardano: ……; ……; …….

Il Responsabile si impegna a trattare i dati personali soltanto su istruzione documentata del Titolare; in particolare, in relazione al rapporto contrattuale di cui in premessa, il Responsabile potrà trattare i dati esclusivamente per finalità di *[specificare la finalità del trattamento]* …….. e potrà effettuare, *[opzione]* con o senza strumenti automatizzati, soltanto le seguenti operazioni: *[specificare le operazioni consentite]* registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, ***[attenzione alla selezione di quelle in riquadro!]*** comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, profilazione**,** cancellazione o distruzione.

Qualora la normativa, comunitaria o nazionale, imponesse al Responsabile il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, lo stesso Responsabile informerà il Titolare di tale obbligo giuridico prima del relativo trasferimento, salvo che la normativa in questione vieti tale informazione per rilevanti motivi di interesse pubblico.

Il Responsabile informerà immediatamente il Titolare qualora, a suo parere, un'istruzione violasse il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Il Responsabile è consapevole ed accetta che i propri dati personali possano essere pubblicati sul sito istituzionale o sulla bacheca del Titolare per finalità di trasparenza nei confronti degli interessati.

Art. 3 – In ogni fase e per ogni operazione del trattamento, il Responsabile dovrà garantire il rispetto dei principi comunitari (ad esempio, di *privacy by design e by default*) e nazionali in ambito di protezione dei dati personali e, in particolare, quelli di cui agli artt. 5 e 25 del Regolamento. Il Responsabile dovrà:

a) garantire che le persone che trattano dati personali siano state specificamente autorizzate, adeguatamente istruite e si siano impegnate alla riservatezza, o abbiano un adeguato obbligo legale di riservatezza;

b) adottare tutte le misure richieste ai sensi dell'articolo 32 del Regolamento, *[da valutare, per alcuni rischi specificamente individuati, in attesa di future prescrizioni]* nonché le misure di sicurezza minime di cui agli artt. 33 e ss. del previgente D. Lgs. 196/03 e relativo Allegato tecnico (B) per i seguenti specifici rischi: …… …….
In caso di trattamento con strumenti automatizzati, il Responsabile garantisce di aver adottato misure di sicurezza analoghe e non inferiori al livello *[opzioni: in relazione alla delicatezza del trattamento e ai costi, scegliere i seguenti livelli]* "minimo"/"standard"/"alto" di cui alla circolare Agid n. 2/2017 (Misure minime di sicurezza ICT per le pubbliche amministrazioni) e successive modifiche e integrazioni;
c) assistere il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (Capo III del Regolamento), nonché informare tempestivamente il Titolare dei reclami eventualmente presentati dagli interessati;
d) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Contratto, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal Titolare, dal suo *Data Protection Officer*, o da un altro soggetto a ciò deputato;
e) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento. In particolare, relativamente alla predisposizione della "valutazione di impatto" ("*Data privacy impact assessment*", di cui agli artt. 35 e 36 del Regolamento), nel caso in cui il Responsabile fornisse al Titolare gli strumenti/applicativi informatici e/o gestisse gli stessi strumenti/applicativi informatici del Titolare, lo stesso sarà tenuto a predisporre ed aggiornare l'analisi dei rischi (probabilità di violazione della sicurezza) degli strumenti/applicativi informatici, comunicandola al Titolare, adottando i criteri di valutazione forniti da quest'ultimo. Con riferimento ai casi di *data breach* (di cui agli artt. 33 e 34 del Regolamento), nel caso in cui gli strumenti/applicativi informatici del Titolare fossero forniti o gestiti dal Responsabile, quest'ultimo è sin d'ora delegato dal Titolare, accettando tale delega senza costi aggiuntivi, ad effettuare la relativa notifica all'Autorità di controllo e comunicazione ai relativi interessati qualora la violazione riguardasse gli strumenti/applicativi informatici stessi; tali adempimenti dovranno essere effettuati previa valutazione, con la struttura provinciale direttamente coinvolta, degli elementi della violazione e delle necessarie conseguenti azioni da intraprendere. Il Responsabile, inoltre, è tenuto a comunicare al Titolare (struttura competente in materia di protezione dei dati

personali), non appena venuto a conoscenza dell'evento, ogni *data breach* che potrebbe ragionevolmente riguardare i dati personali che tratta per conto del Titolare;

f) nei casi prescritti dall'art. 37 del Regolamento, *[opportuno]* oltre che nelle fattispecie in cui tale adempimento sia raccomandato nelle specifiche Linee Guida del Gruppo di Lavoro Art. 29, provvedere alla nomina del *Data Protection Officer* (di seguito, "DPO"), nel rispetto dei criteri di selezione stabiliti dallo stesso Regolamento, dalle relative Linee Guida del Gruppo di Lavoro Art. 29, nonché dalle indicazioni fornite dalla Autorità di controllo, garantendo il rispetto delle prescrizioni di cui all'art. 38, anche allo scopo di consentire al medesimo DPO l'effettivo adempimento dei compiti di cui all'art. 39 del Regolamento;

g) provvedere alla designazione per iscritto del/degli Amministratore/i di Sistema secondo i criteri di individuazione e selezione previste dall'Autorità di controllo con provvedimento dd. 27/11/2008 e s.m.i., conservando l'elenco degli stessi Amministratori, verificandone annualmente l'operato ed adottando sistemi idonei alla registrazione dei relativi accessi logici (da conservare con caratteristiche di inalterabilità e integrità per almeno per 6 mesi). Qualora l'attività degli stessi Amministratori di Sistema riguardasse, anche indirettamente, servizi o sistemi che trattano, o che permettono il trattamento, di informazioni di carattere personale dei dipendenti del Titolare, comunicare a quest'ultimo l'identità degli Amministratori di Sistema (provvedendo a dare idonea informativa, *ex* art. 13 del Regolamento, agli stessi Amministratori);

h) provvedere alla predisposizione del Registro delle attività del trattamento nei termini di cui all'art. 30 del Regolamento, mettendolo tempestivamente a disposizione del Titolare, o dell'Autorità di controllo, in caso di relativa richiesta;

i) comunicare, al Titolare, i nominativi di riferimento per l'esecuzione del Contratto, nonché il nominativo dell'eventuale DPO;

j) alla scadenza del rapporto contrattuale di cui in premessa (ivi compresi i casi di risoluzione o recesso), o al più al termine dell'esecuzione delle relative attività/prestazioni e, quindi, delle conseguenti operazioni di trattamento, fatta salva una diversa determinazione del Titolare, dovrà provvedere alla cancellazione (ivi compresa ogni eventuale copia esistente) dei dati personali in oggetto (dandone conferma scritta al Titolare), a meno che la normativa comunitaria o nazionale ne preveda la conservazione ed esclusa ogni altra forma di conservazione anche per finalità compatibili. In caso di trattamento con modalità automatizzate, il Responsabile garantisce che, su richiesta del Titolare e senza costi aggiuntivi, prima di effettuare la cancellazione predetta potrà effettuare la trasmissione sicura dei dati personali ad altro soggetto, in un formato

strutturato, di uso comune e leggibile da dispositivo automatico, beninteso qualora il destinatario sia attrezzato a riceverli.

Art. 4 - Il Responsabile non ricorrerà ad altro ulteriore Responsabile del trattamento (di seguito il ("*sub-Responsabile*") senza previa autorizzazione scritta, specifica o generale, del Titolare. Nel caso di autorizzazione scritta generale, il Responsabile informerà il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di ulteriori sub-Responsabili, dando così al Titolare l'opportunità di opporsi a tali modifiche. In ogni caso, qualora il Responsabile ricorresse ad un sub-Responsabile per l'esecuzione di specifiche attività di trattamento per conto del Titolare, dovrà sottoscrivere, con tale sub-Responsabile, un contratto (o altro atto giuridico) analogo al presente Contratto – stipulato in forma scritta, anche in formato elettronico – imponendo a quest'ultimo gli stessi obblighi in materia di protezione dei dati contenuti nel presente Contratto (e in ogni altro atto giuridico o *addendum* intervenuto tra le Parti) e prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento, nonché della relativa disciplina nazionale.
Qualora i dati personali fossero trasferiti verso Paesi terzi ovvero organizzazioni internazionali, il Responsabile dovrà garantire il rispetto delle condizioni di cui agli art. 44 e ss. del Capo V del Regolamento. Resta inteso che, laddove il sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile sarà ritenuto integralmente responsabile nei confronti del Titolare dell'adempimento degli obblighi del sub-Responsabile.

Art. 5 – In caso di azione di risarcimento civile, o responsabilità amministrativa, promossa nei confronti del Titolare per i danni provocati, o le violazioni commesse dal Responsabile a seguito di inadempienze normative o contrattuali, il Responsabile stesso manleva integralmente il Titolare, ogni eccezione rimossa. Analogamente, il Responsabile manleva integralmente il Titolare, ogni eccezione rimossa, in caso di applicazione di sanzioni da parte dell'Autorità di controllo per inadempienze normative o contrattuali commesse dallo stesso Responsabile.

Art. 6 – Il Contratto avrà termine il …… *[inserire lo stesso termine del rapporto contrattuale principale]*; in forza del collegamento con il/la contratto/convenzione di cui in premessa, la risoluzione o il recesso del/della stesso/a contratto/convenzione produrrà

medesimo effetto sul presente Contratto.

Art. 7 – Per ogni controversia riguardante il presente Contratto è competente il Foro di Trento.

Provincia autonoma di Trento ……

…… ……

Il Responsabile, ai sensi e per gli effetti dell'art. 1341 c.c., accetta e sottoscrive espressamente le seguenti clausole:

Art. 1 – diligenza professionale

Art. 4 – restrizione alla libertà contrattuale nei rapporti coi terzi

Art. 5 – limitazione di responsabilità (manleva)

Art. 7 – Foro competente

……

Mod. (A.1)
Ed. 1-2019

Sig……...

Nota Prot.……

AUTORIZZAZIONE AL TRATTAMENTO

***ex* artt. 29 e 32 del Reg. UE 2016/679 – art. 2-*quaterdecies* D. Lgs. 196/03**

Premesso che:

- La Provincia autonoma di Trento è *Titolare del trattamento* (di seguito, il "*Titolare*") dei dati funzionali all'esercizio delle proprie competenze istituzionali;

- L'art. 29 del Regolamento UE 2016/679 (di seguito, il "Regolamento") prevede che "*...chiunque agisca sotto la... autorità... del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*";

- l'art. 2-*quaterdecies* del D. Lgs. 196/03 stabilisce che "1. *Il titolare o il responsabile del trattamento possono prevedere, nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche espressamente designate che operano sotto la loro autorità. 2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità";*

- i Dirigenti delle strutture provinciali, in qualità di *Preposti al trattamento*, provvedono, in nome e per conto della Provincia, ad autorizzare al trattamento dei dati personali

Il sottoscritto

…….

nel nominarLa "*Addetto al trattamento*",

La autorizza al trattamento stesso,

dei dati personali, compresi, eventualmente, quelli riconducibili alle particolari categorie (di cui all'art. 9 del Regolamento) e quelli relativi a condanne penali e reati (di cui all'art. 10 del Regolamento), anche contenuti nei relativi archivi, effettuati sia con strumenti elettronici sia senza strumenti elettronici, strettamente necessari per l'adempimento dei compiti e funzioni a Lei affidati.

Il/i trattamento/i a lei pertinente/i, in particolare, è/sono contraddistinto/i (nel Registro elettronico dei trattamenti, al quale si rinvia per le specifiche) con sigla: T……; T……..; T……..

Le ricordiamo che il soggetto autorizzato opera sotto la diretta autorità del *Preposto al trattamento* (di seguito il "*Preposto*") ed è tenuto al rigoroso rispetto dei principi del Regolamento, del Decreto Legislativo 196/03, dei Codici Deontologici/Regole Deontologiche, del regolamento dei dati sensibili e giudiziari (D.P.P. n. 27-129/Leg. dd. 8/10/2013 e s.m.i.), dei Provvedimenti e Linee Guida del Garante e del Comitato europeo per la protezione dei dati, degli eventuali Codici di Condotta o Certificazioni a cui il *Titolare* abbia aderito, del Codice di comportamento provinciale e della normativa di settore, nonché ad attenersi alle circolari interne e alle deliberazioni della Giunta Provinciale in materia di privacy e in materia di uso degli strumenti informatici e posta elettronica, alla *policy* in materia di sicurezza informatica, oltre che alle restanti istruzioni impartite dal *Titolare* o dal *Preposto*. Nel caso di mancato rispetto delle istruzioni e delle *policy* aziendali si applicheranno le sanzioni disciplinari previste dal contratto nazionale.

La informiamo, inoltre, che l'accesso e la permanenza nei sistemi informatici aziendali per ragioni estranee o, comunque, diverse rispetto a quelle per le quali è stato abilitato, può integrare il reato di accesso abusivo ai sistemi informatici, esponendo l'ente a danni reputazionali che possono comportare gravi sanzioni disciplinari a Suo carico.

Si ritiene doveroso precisare che la presente nomina non comporterà alcuna modifica della qualifica professionale o delle mansioni assegnate. La nomina può essere conosciuta dagli *interessati* e sarà conservata nel Registro elettronico dei trattamenti e agli atti dell'ufficio nel rispetto del principio di *accountability*.

Nella qualità di *Addetto al trattamento*, Lei sarà periodicamente tenuto a partecipare a seminari e corsi di formazione in materia di protezione dei dati personali.

Di seguito, vengono elencate le principali istruzioni per il trattamento dei dati personali.

Regole generali per tutti i trattamenti

Il trattamento dei dati, ai sensi degli artt. 5 e 25 del Regolamento, deve rispettare il principio di "minimizzazione" (un tempo definito di "pertinenza e non eccedenza"), ovvero di limitazione (a) della quantità e qualità dei dati personali trattati, (b) delle operazioni di trattamento compiute sugli stessi, (c) di conoscibilità degli stessi dati e (d) di conservazione dei dati medesimi, in riferimento alle finalità del trattamento. Pertanto, è consentito l'accesso ai soli dati personali la cui conoscenza sia strettamente indispensabile per adempiere ai compiti affidati.

I dati devono essere trattati in modo lecito, corretto e trasparente, ed essere esatti ed aggiornati.

L'*Addetto al trattamento* (di seguito, l'"*Addetto*"), in particolare, nello svolgimento del trattamento, è tenuto a:

- accertare che l'informativa, completa in tutte le sue parti, venga consegnata all'*interessato*, ai sensi degli artt. 13 e 14 del Regolamento, e verificare che ciascuna particolare operazione del trattamento (quali, ad esempio, la comunicazione e diffusione dei dati, ovvero la profilazione), sia conforme alle disposizioni di legge e di regolamento;
- assicurare l'esercizio dei diritti e delle facoltà previste dagli artt. 15, 16, 17, 18, 21, 22 e 26 del Regolamento (diritto di accesso; diritto di rettifica; diritto alla cancellazione; diritto di limitazione, diritto di opposizione; diritto di intervento umano e contestazione in caso di decisione basata esclusivamente su trattamento automatizzato; di accedere al contenuto essenziale del contratto di contitolarità);
- collaborare, con gli altri *Addetti* al medesimo trattamento, esclusivamente per le finalità dello stesso e nel rispetto delle indicazioni fornite;
- non trasmettere, a *terzi*, informazioni circa i dati personali trattati. La comunicazione e la diffusione è ammessa soltanto se funzionale allo svolgimento dei compiti affidati, o in forza di obblighi normativi, comunque previa autorizzazione del *Preposto*;
- accertarsi dell'identità dell'*interessato*, prima di fornire informazioni circa i suoi dati personali o il relativo trattamento effettuato;

- se, per lo svolgimento dei compiti ed attività affidate, è doveroso accertare l'identità dell'*interessato*, ma senza alcuna necessità di mantenere copia del documento identificativo dell'interessato, limitarsi alla verifica dello stesso documento;
- riporre in archivio, al termine del periodo di trattamento, i supporti o i documenti, ancorché non definitivi (bozze), contenenti i dati personali;
- non lasciare incustodite, presso le fotocopiatrici, le stampe di documenti contenti dati personali;
- qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili;
- conservare i dati trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati, nel rispetto dei termini normativamente previsti (e dal "massimario di scarto");
- in caso di dubbio in materia di trattamento dei dati personali, rivolgersi al proprio *Referente* privacy;
- segnalare immediatamente al *Preposto* eventuali anomalie, incidenti, furti, perdite accidentali di dati connessi con una ricaduta sul trattamento dei dati personali, al fine di attivare le procedure di comunicazione delle violazioni di dati (*data breach*) al Garante e agli *interessati.*

Si rammenta che la consultazione dei dati contenuti nelle banche dati (archivi), non consente alcuna forma di comunicazione, diffusione e ulteriore trattamento degli stessi che non sia strettamente necessario e funzionale all'espletamento dei compiti e delle funzioni attribuite. I dati "pubblici", ovvero conoscibili da parte di chiunque, non legittimano gli *Addetti* alla comunicazione o diffusione degli stessi.

Per quanto riguarda i flussi di documenti tra le strutture provinciali, devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse).

Nel caso di presenza di ospiti o personale di servizio, inoltre sarà necessario:

- fare attendere gli ospiti o il personale di servizio in luoghi in cui non sono presenti informazioni riservate, o dati personali, abbassando il tono di voce o chiudendo le porte in caso di comunicazioni verbali, o telefoniche;
- evitare di allontanarsi dalla scrivania, o riporre i documenti e attivare il salvaschermo del PC;
- la *password* è personale e dev'essere mantenuta segreta e custodita, nel rispetto delle misure di sicurezza stabilite dalle deliberazioni della Giunta provinciale; pertanto, è doveroso non rivelare o far digitare la *password* al personale di assistenza tecnica;
- non rivelare le *password* al telefono, ne inviarle via *fax*; nessuno è autorizzato a chiederle;
- segnalare qualsiasi anomalia al *Preposto*.

Trattamenti concernenti particolari categorie (di cui all'art. 9 del Regolamento)

e quelli relativi a condanne penali e reati (di cui all'art. 10 del Regolamento)

Fermo il rispetto di quanto sin qui previsto, per il trattamento dei dati personali di cui al presente paragrafo, si prescrivono le seguenti ulteriori istruzioni:

- non fornire tali dati personali per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- evitare di inviare, per *fax*, documenti in chiaro contenenti tali dati: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'*interessato* (ad esempio, contrassegnando i documenti semplicemente con un codice);
- i documenti, ancorché non definitivi, ed i supporti recanti tali dati, devono essere conservati, anche in corso di trattamento, in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza dell'*Addetto*;
- in relazione alle specifiche esigenze e finalità del trattamento, valutare attentamente se richiedere il certificato del casellario giudiziale, oppure quello dei carichi pendenti;

- i supporti e i documenti recanti dati relativi alla salute, alla vita sessuale e all'orientamento sessuale, genetici e biometrici devono essere conservati nei predetti contenitori muniti di serratura, separatamente da ogni altro documento.

Trattamenti con strumenti elettronici

Per quanto riguarda, in particolare, le elaborazioni e le altre fasi dei trattamenti effettuate attraverso strumenti informatici, l'*Addetto* disporrà di una parola chiave strettamente personale per l'accesso ai dati e di un proprio codice identificativo.

L'*Addetto* avrà cura di:

- non condividere il proprio codice identificativo personale con altri utenti, salvo i casi espressamente previsti;
- non cedere a terzi la propria parola chiave di autenticazione;
- non accedere a servizi non consentiti;
- non caricare ed eseguire *software* ulteriori rispetto a quelli istituzionali, senza previa verifica da parte del proprio Referente informatico;
- non collegare dispositivi che consentano un accesso, non controllabile, ad apparati di rete della Provincia;
- memorizzare i dati di interesse lavorativo sui dischi U e Y, ove disponibili; in caso contrario, effettuare il *backup* periodico per i trattamenti non gestiti da Trentino Digitale S.p.a.;
- procedere alla cancellazione dei supporti magnetici od ottici contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, gli stessi devono essere distrutti.

Nel caso di trasferimento, anche temporaneo, ad altra struttura/ufficio, o nell'ipotesi di cessazione del rapporto di lavoro, l'*Addetto* perde i privilegi di accesso ai dati personali attribuiti all'ufficio di provenienza.

Data _____

Firma

Il DIRIGENTE (*Preposto al trattamento*)

Firma, per presa visione,

L'*Addetto al trattamento*

DICHIARAZIONE DI RISERVATEZZA

Preso atto di tutto quanto sopra, consapevole delle responsabilità che assume, l'*Addetto*, anche in forza di quanto previsto all'art. 28, par. 3, lett. b), del Regolamento, si impegna a:

- mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le relative informazioni, anche ai sensi del Codice di comportamento;

- non comunicare a terzi, o diffondere, le notizie, le informazioni e i dati personali conosciuti in relazione a fatti e circostanze apprese nella propria qualità di dipendente, o per effetto delle attività svolte per il *Titolare*.

L'*Addetto al trattamento*

_____

Mod. (N.A.1)
Ed. 1-2019

OGGETTO: Nomina ad "Amministratore di Sistema", ai sensi del provvedimento a carattere generale del Garante per la protezione dei dati personali del 27 novembre 2008 (G.U. n. 300 dd. 24/12/2008) e s.m.i.

La Provincia autonoma di Trento, *Titolare del trattamento* dei dati personali ai sensi dell'art. 4, § 7), del Regolamento UE 2016/679, nella persona del *Preposto al trattamento* (Dirigente), Sig./Sig.ra ……., considerato:

- il rapporto di lavoro con Lei in vigore, la sua qualifica e la documentata preposizione alla unità operativa di appartenenza;

- che le prestazioni da Lei effettuate, in via ordinaria, forniscono idonea garanzia del pieno rispetto delle caratteristiche di esperienza, capacità e affidabilità, nonché delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

- che Lei è professionalmente preposto alla gestione e/o manutenzione di un impianto di elaborazione e/o di sue componenti,

La nomina,

"Amministratore di Sistema"

per i trattamenti svolti per conto della Provincia, con riguardo agli ambiti e ai compiti riportati, a titolo esemplificativo, nello schema seguente (quale "*elencazione analitica*" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato):

…….	……...	……..	……..

Descrizione	Dati elettronici	Ambito	Operatività
……...	……...	……...	……...
Tipologia di Amministratore	*dati in oggetto*	*data base*	*attività dell'Amministratore*
……..	……..	……...	……...
Esempio: Amministratore di sistema software	*Software, informazioni gestite da applicativi e servizi*	*DB-ABC*	*Installazione e gestione delle singole postazioni e aree di lavoro, di software di base, aggiornamenti, backup; Manutenzione e configurazione server di produzione*

Specificatamente e limitatamente a tale contesto, l'Amministratore di Sistema deve assicurare il corretto funzionamento e utilizzo del sistema informatico oggetto dell'incarico.

Con l'occasione La informo, altresì, che:

- ai sensi del punto 2, lett. c), del provvedimento del Garante per la protezione dei dati personali del 27/11/2008, il *Titolare del trattamento*, per finalità di trasparenza interna all'organizzazione, è tenuto, a tutela dei lavoratori, ad instaurare un regime di conoscibilità dell'identità degli Amministratori di Sistema;

- ai sensi del punto 2, lett. e), del provvedimento del Garante per la protezione dei dati personali del 27/11/2008, l'operato degli Amministratori di Sistema deve essere oggetto, da parte del *Titolare del trattamento* o dei *Preposti*, di una attività di verifica, con cadenza almeno annuale, sull'attività svolta in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti;
- ai sensi del punto 2, lett. f), del provvedimento del Garante per la protezione dei dati personali del 27/11/2008, devono essere registrati gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema.

_____

Firma Preposto

(Dirigente)

Il sottoscritto dichiara di accettare la nomina ad Amministratore di Sistema, con riguardo agli ambiti e ai compiti sopra descritti, dichiarandosi, altresì, disponibile e competente per la piena attuazione di quanto ivi disposto.

Data _____

PER ACCETTAZIONE

_____

Mod. (D.B. 1)
Ed. 1-2018

NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) AL GARANTE (*ex* art. 33 Reg. UE 2016/679)

Amministrazione Titolare del trattamento

Denominazione

Provincia

Comune

Cap

Indirizzo

Nome e Cognome del Responsabile della struttura organizzativa che ha subito la violazione

Nome e Cognome della persona fisica addetta alla comunicazione

Funzione rivestita

Recapito telefonico per eventuali comunicazioni

Indirizzo PEC e/o EMAIL per eventuali comunicazioni

Responsabile esterno del trattamento

Denominazione

Provincia

Comune

Cap

Indirizzo

Nome e Cognome del Responsabile della struttura organizzativa che ha subito la violazione

Nome e Cognome della persona fisica addetta alla comunicazione

Funzione rivestita

Recapito telefonico per eventuali comunicazioni

Indirizzo PEC e/o EMAIL per eventuali comunicazioni

Responsabile protezione dati

Nominativo

Recapito telefonico per eventuali comunicazioni

Indirizzo PEC e/o EMAIL per eventuali comunicazioni

DESCRIZIONE DELLA NATURA DELLA VIOLAZIONE DEI DATI

Quando si è verificata la violazione dei dati personali

Il

Tra il e il

In un tempo non ancora determinato

È possibile che sia ancora in corso

Dove è avvenuta la violazione?

[Specificare, ad es., se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili]

Modalità di esposizione al rischio

[rischi che derivano dalla perdita di: riservatezza, integrità e disponibilità]

1) Tipo di violazione

Lettura (presumibilmente i dati non sono stati copiati)

Copia (i dati sono ancora presenti sui sistemi del Titolare)

Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

Cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione)

Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)

Altro

2) Dispositivo oggetto della violazione

Computer

Rete

Dispositivo mobile

File o parte di un file

Strumento di backup

Documento cartaceo

Altro (es. Archivio fisico)

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

Quante persone sono state colpite dalla violazione dei dati personali trattati

N__persone

Circa___persone

Un numero (ancora) sconosciuto di persone

Che tipo di dati sono stati oggetto di violazione

Dati anagrafici/codice fiscale

Dati di accesso e identificazione (user name, password, customer ID, altro)

Dati relativi a minori

Dati relativi all'ubicazione di persone fisiche

Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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

Dati relativi a condanne penali e reati

Copia per immagine su supporto informatico di documenti analogici

Ancora sconosciuto

Altro _____

Livello di gravità della violazione per i diritti e le libertà dell'interessato

Basso/trascurabile

Medio

137

Alto

Molto alto

PROBABILI CONSEGUENZE DELLA VIOLAZIONE DEI DATI

[esempio: furto di identità; perdite finanziarie; danni all'immagine, ecc.]

MISURE TECNICHE ED ORGANIZZATIVE

Misure tecniche ed organizzative applicate ai dati oggetto di violazione

Misure tecniche ed organizzative che sono state adottate, successivamente al *data breach*, per contenere la violazione dei dati e attenuare i possibili effetti negativi

COMUNICAZIONI AGLI INTERESSATI

La violazione è stata comunicata anche agli interessati?

Si, è stata comunicata il

No, perché

Contenuto della comunicazione resa agli interessati

Mod. (D.B. 2)
Ed. 1-2018

COMUNICAZIONE DI VIOLAZIONE DEI DATI PERSONALI (*DATA BREACH*) ALL'INTERESSATO (*ex* art. 34 Reg. UE 2016/679)

Egr./Gent. Sig./Sig.ra

La informiamo che il nostro Ente ha subito un ..... *[descrizione dell'evento, ad es: attacco informatico, furto, danneggiamento, ecc.]* che ha comportato una violazione dei Suoi dati.

Dai primi accertamenti in corso, pare che la violazione abbia natura *[accidentale / dolosa]*.

Di seguito le forniamo alcune informazioni a riguardo, restando a Sua disposizione per ulteriori chiarimenti al seguente "punto di contatto".

Amministrazione Titolare del trattamento

Denominazione

Provincia

Comune

Cap

Indirizzo

Nome e Cognome del Responsabile della struttura organizzativa che ha subito la violazione

Nome e Cognome della persona fisica addetta alla comunicazione (e punto di contatto)

Funzione rivestita

Recapito telefonico per eventuali comunicazioni

Indirizzo PEC e/o EMAIL per eventuali comunicazioni

Responsabile esterno del trattamento

Denominazione

Provincia

Comune

Cap

Indirizzo

Nome e Cognome del Responsabile della struttura organizzativa che ha subito la violazione

Nome e Cognome della persona fisica addetta alla comunicazione (e punto di contatto)

Funzione rivestita

Recapito telefonico per eventuali comunicazioni

Indirizzo PEC e/o EMAIL per eventuali comunicazioni

Responsabile protezione dati

Nominativo

Recapito telefonico per eventuali comunicazioni

Indirizzo PEC e/o EMAIL per eventuali comunicazioni

DESCRIZIONE DELLA NATURA DELLA VIOLAZIONE DEI DATI

Quando si è verificata la violazione dei dati personali

Il

Tra il e il

In un tempo non ancora determinato

È possibile che sia ancora in corso

Quante persone sono state colpite dalla violazione dei dati personali trattati

N__persone

Circa___persone

Un numero (ancora) sconosciuto di persone

Che tipo di dati sono stati oggetto di violazione

Dati anagrafici/codice fiscale

Dati di accesso e identificazione (user name, password, customer ID, altro)

Dati relativi a minori

Dati relativi all'ubicazione di persone fisiche

Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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

Dati relativi a condanne penali e reati

Copia per immagine su supporto informatico di documenti analogici

Ancora sconosciuto

Altro (ad es. Archivio fisico)

PROBABILI CONSEGUENZE DELLA VIOLAZIONE DEI DATI

[esempio: furto di identità; perdite finanziarie; danni all'immagine, ecc.]

MISURE TECNICHE ED ORGANIZZATIVE

Misure tecniche ed organizzative applicate ai dati oggetto di violazione

Misure tecniche ed organizzative che sono state assunte, successivamente al *data breach*, per contenere la violazione dei dati e attenuare i possibili effetti negativi

Misure che si raccomanda all'interessato di adottare, per porre rimedio alle probabili conseguenze delle violazioni e per attenuarne i possibili effetti negativi

.....