PARCO NATURALE ADAMELLO BRENTA
STREMBO

Documento programmatico sulla sicurezza

Redatto in base alle disposizioni di cui al punto 19 del
DISCIPLINARE TECNICO IN MATERIA DI MISURE
MINIME DI SICUREZZA del
CODICE IN MATERIA DI DATI PERSONALI
(D.lgs. n.196 del 30 giugno 2003)

Prot. n. 1178/I/14/3

IL PRESIDENTE
f.to Antonio Caola

Strembo, 24 marzo 2014

1) DISPOSIZIONI GENERALI

1.1. Riferimenti normativi

CODICE IN MATERIA DI DATI PERSONALI (D.lgs. n. 196 del 30 giugno 2003)
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice – Allegato B)

1.2. Scopo

Il presente Documento Programmatico sulla Sicurezza è redatto per soddisfare tutte le misure minime di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali conformemente a quanto previsto dal Codice in materia di protezione dei dati personali (Decreto legislativo 30.06.2003 n. 196). Costituisce inoltre un valido strumento per l'adozione delle misure idonee previste dall'art. 31 dallo stesso Codice e dal Disciplinare Tecnico in materia di misure minime di sicurezza.
Grazie al presente Documento Programmatico sulla Sicurezza è possibile ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato, o di trattamento non consentito o non conforme alle formalità di raccolta, intendendosi, come misure di sicurezza, il complesso degli accorgimenti tecnici, informatici, organizzativi e logistici e procedurali di sicurezza.
Il Documento verrà reso disponibile per la lettura al personale dipendente e agli amministratori del Parco Naturale Adamello Brenta.

1.3. Campo di applicazione

Il Documento Programmatico sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali del Parco Naturale Adamello Brenta con sede in Strembo.
Tale documento riguarda il trattamento di tutti i dati personali

- Sensibili
- Comuni
- Giudiziari

Il DPS si applica al trattamento di tutti i dati personali per mezzo di

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (cartacei, audio, visivi, audiovisivi, ecc…)

Il contenuto deve essere divulgato e spiegato a tutti gli incaricati, conosciuto ed applicato da tutte le funzioni che fanno parte del Parco Naturale Adamello Brenta.

1.4. Revisione del documento

Entro il 31 marzo di ogni anno il Titolare del trattamento dati deve verificare ed eventualmente predisporre un aggiornamento del DPS contenente idonee informazioni riguardo ai punti 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7 e 19.8 del Disciplinare tecnico in materia di misure minime di sicurezza.

1.5. Definizioni

I termini titolare, responsabile, incaricato, interessato, ecc…, sono quelli stabiliti dall'art. 4 del Codice.

1.5.1. Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

1.5.2. Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

1.5.3. Dati sensibili

I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

1.5.4. Dati giudiziari

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, 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.

1.5.5. Titolare

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

1.5.6. Responsabile

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

1.5.7. Incaricati

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

1.5.8. Interessato

La persona fisica, la persona giuridica, l'ente o l'associazione a cui si riferiscono i dati personali.

1.5.9. Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.5.10. Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.5.11. Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

1.5.12. Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

1.5.13. Banca dati

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

1.5.14. Comunicazione elettronica

Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.
Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

1.5.15. Misure minime

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

1.5.16. Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

1.5.17. Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche diretta dell'identità.

1.5.18. Credenziali di autorizzazione

I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

1.5.19. Parola chiave

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

1.5.20. Profilo di autorizzazione

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essi consentita.

1.5.21. Sistema di autorizzazione

L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

2) RUOLI, COMPITI E NOMINA DELLE FIGURE PREVISTE PER LA SICUREZZA DEI DATI PERSONALI

2.1. Titolare del trattamento dati personali. Compiti.

Il titolare del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad un altro titolare, le decisioni in ordine alle formalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Deve assicurare e garantire direttamente che vengano adottate tutte le misure di sicurezza ai sensi del codice in materia di Dati personali e del Disciplinare Tecnico in materia di misure minime di sicurezza tese a ridurre al minimo il rischio di distruzione dei Dati, accesso non autorizzato o trattamento non consentito previe idonee istruzioni fornite per iscritto.
Può nominare, se lo ritiene opportuno, uno o più responsabili del trattamento dati. Qualora non ritenga di nominare alcun responsabile ne assumerà tutte le responsabilità e le funzioni.
Titolare del Trattamento dati è il Parco Naturale Adamello Brenta con sede in Strembo.

2.2. Responsabile della sicurezza e del trattamento dei dati personali

La nomina di ciascun Responsabile della sicurezza e del trattamento deve essere effettuata dal Titolare con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.
Il Titolare deve informare il Responsabile della sicurezza e del trattamento delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (D.lgs. n. 196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il Titolare deve consegnare al Responsabile della sicurezza e del trattamento una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del Responsabile della sicurezza e del trattamento è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

Il Responsabile della sicurezza e del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che ha il compito di individuare, nominare e incaricare per iscritto, gli Incaricati del trattamento dei dati personali.
Il Responsabile della sicurezza e del trattamento dei dati personali ha il compito di:

- nominare gli incaricati del trattamento per le Banche di dati che gli sono state affidate;
- sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali;
- dare le istruzioni adeguate agli incaricati del trattamento effettuato con strumenti elettronici e non;
- verificare periodicamente, o comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali;
- garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- redigere ed aggiornare ad ogni variazione l'elenco delle sedi e gli uffici in cui vengono trattati i dati;
- redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento;
- se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione;
- definire e verificare periodicamente le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- qualora il trattamento dei dati sia effettuato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto uno o più incaricati della gestione e della manutenzione degli strumenti elettronici (amministratore di sistema);
- se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto uno o più incaricati della custodia delle copie delle credenziali qualora vi sia più di un incaricato del trattamento;
- se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto uno o più incaricati delle copie di sicurezza delle banche dati.

Responsabile del trattamento dati del Parco Naturale Adamello Brenta è il Direttore dott. Roberto Zoanetti.

2.3. Incaricato del trattamento dei dati personali

La nomina di ciascun Incaricato del trattamento deve essere effettuata dal Responsabile della sicurezza e del trattamento dei dati o dal Titolare del trattamento dati, con una lettera di incarico in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata per presa visione.
Il Responsabile della sicurezza e del trattamento deve informare ciascun Incaricato del trattamento dei dati personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI

(D.lgs. n.196 del30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.
Il Responsabile della sicurezza e del trattamento deve consegnare a ciascun Incaricato del trattamento dei dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
Gli Incaricati del trattamento dei dati personali devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.
Agli Incaricati del trattamento dei dati personali devono essere assegnate una parola chiave e un codice di autenticazione informatica.
Agli Incaricati del trattamento dei dati personali è prescritto di adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.
Gli Incaricati del trattamento sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali da un Responsabile del trattamento.
In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- Gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza la parola chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
- La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'incaricato del trattamento deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.
- Gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazioni, e sono restituiti al termine delle operazioni affidate.

Gli incaricati del trattamento dati per il Parco Naturale Adamello Brenta sono:

- personale amministrativo
- personale tecnico
- personale generico
- guardaparco
- borsisti, stagisti e tesisti

come risulta dall'elenco allegato al presente documento.

2.4 Incaricato delle copie di sicurezza delle banche dati

Il Responsabile della sicurezza e del trattamento dei dati o il Titolare del trattamento dati, nomina uno o più soggetti Incaricati delle copie di sicurezza delle banche dati a cui è conferito il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

Il Responsabile della sicurezza e del trattamento dei dati deve informare ciascun Incaricato delle copie di sicurezza delle banche dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (D.lgs. n. 196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA MISURE MINIME DI SICUREZZA.

La nomina di uno o più Incaricati delle copie di sicurezza delle banche dati deve essere effettuata con una lettera di incarico e deve essere controfirmata per accettazione.

Il Responsabile della sicurezza e del trattamento dei dati deve consegnare a ciascun Incaricato delle copie di sicurezza delle banche dati una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

L'Incaricato delle copie di sicurezza delle banche dati è la persona fisica o la persona giuridica che ha il compito di sovrintendere all'esecuzione periodica delle copie di sicurezza delle Banche di dati personali gestite.

È onere del Responsabile della sicurezza e del trattamento dei dati, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati delle copie di sicurezza delle banche dati.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce, con il supporto tecnico dell'Amministratore di sistema la periodicità con cui debbono essere eseguite le copie di sicurezza delle Banche di Dati trattate. I criteri debbono essere concordati con l'Amministratore di sistema in relazione al tipo di rischio potenziale e al livello di tecnologia utilizzata.

In particolare per ogni Banca di dati debbono essere definite le seguenti specifiche:

- il "Tipo di supporto" da utilizzare per le "Copie di Back-up";
- il numero di "Copie di Back-up" effettuate ogni volta;
- se i supporti utilizzati per le "Copie di Back-up" sono riutilizzati e in questo caso con quale periodicità;
- se per effettuare le "Copie di Back-up" si utilizzano procedure automatizzate e programmate;
- le modalità di controllo delle "Copie di Back-up";
- la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- l'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-up";
- le istruzioni e i comandi necessari per effettuare "Copie di Back-up".

È compito degli Incaricati delle copie di sicurezza delle banche dati:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Responsabile del trattamento dei dati;
- assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro;

- assicurarsi della conservazione delle copie di sicurezza dei dati in luogo adatto e sicuro e ad accesso controllato;
- provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato;
- segnalare tempestivamente all'Amministratore di sistema, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Incaricato della custodia delle copie di sicurezza delle banche dati del Parco Naturale Adamello Brenta è il Signor Periotto rag. Flavio, nominato con lettera prot. n. 6207/I/14/3 di data 11 dicembre 2009.

2.5 Incaricato del trattamento dei dati relativi al personale dipendente e collaboratori vari.

La nomina dell'Incaricato del trattamento dei dati relativi al personale dipendente e ai collaboratori deve essere effettuata dal Responsabile della sicurezza e del trattamento dei dati o dal Titolare del trattamento dati, con una lettera di incarico in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata per presa visione.

Il Responsabile della sicurezza e del trattamento deve informare l'Incaricato del trattamento dei dati relativi al personale dipendente e ai collaboratori delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (D.lgs. n. 196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

All'Incaricato in parola è prescritto di adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

In particolare l'Incaricato del trattamento dei dati relativi al personale dipendente e ai collaboratori deve osservare le seguenti disposizioni:

- deve conservare con la massima segretezza la parola chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- l'incaricato del trattamento deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi;
- in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
- l'incaricato del trattamento non deve in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- l'incaricato del trattamento deve controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati all'incaricato del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi

dall'incaricato fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazioni, e sono restituiti al termine delle operazioni affidate.

Incaricato del trattamento dei dati relativi al personale dipendente e collaboratori vari è la Signora Caola rag. Carmen, nominata con lettera prot. n. 1469/I/14/3 di data 31 marzo 2008.

2.6 Amministratore di Sistema.

In base a quanto stabilito dal Provvedimento a carattere generale del 27.11.2008 pubblicato nella G.U. n. 300 del 24.12.2008, il Titolare del Trattamento, in presenza di sistemi software complessi, deve designare uno o più soggetti Amministratori di Sistema, Amministratori di base dati e Amministratori di rete anche mediante suddivisione dei compiti, laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali.

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai seni dell'articolo 30 del Codice, il titolare ed il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'articolo 29.

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

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 sistemi informatici con cui sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'articolo 3 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 01.03.2007 (in G.U. 10.3.2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (intranet, ordini di servizio a circolazione interna o bollettini). Ciò salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di una eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche

e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.
Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore ai sei mesi.

L'Amministratore di sistema ha il compito di:

- redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione;
- individuare, nominare ed incaricare per iscritto uno o più incaricati alla gestione e della manutenzione degli strumenti elettronici;
- ai sensi del Provvedimento del Garante del 27.11.2008, comma 2 lettera f, adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore ai sei mesi.

L'Ente Parco Naturale Adamello Brenta sulla propria rete informatica non detiene alcun file relativo a dati sensibili.

L'Amministratore di base dati ha il compito di:

- individuare, nominare e incaricare per iscritto uno o più incaricati delle copie di sicurezza delle banche dati;
- individuare, nominare e incaricare per iscritto uno o più incaricati della custodia delle copie delle credenziali;
- custodire e conservare i supporti utilizzati per le copie dei dati;
- ai sensi del Provvedimento del Garante del 27.11.2008, comma 2 lettera f, adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore ai sei mesi.

L'Amministratore di rete ha il compito di:

- Gestire e mantenere le connessioni di rete aziendali, garantendone la funzionalità e la sicurezza specie nei contesti nei quali queste siano interfacciate con altre reti pubbliche o private.

Qualora il titolare del trattamento ritenga di non nominare alcun Amministratore di sistema, Amministratore di base dati, Amministratore di rete, ne assumerà tutte le responsabilità e funzioni.
Il titolare del trattamento informa che ha la facoltà di prevenire ed accertare eventuali accessi non consentiti ai dati personali e con cadenza per lo meno annuale verificare la rispondenza dell'operato dell'Amministratore di rete in

merito alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali.
Viene precisato inoltre che se l'incarico di Amministratore di sistema, Amministratore di base dati, Amministratore di rete è affidato in outsourcing, il titolare del trattamento ai sensi del provvedimento del Garante del 27.11.2008 comma 2 lettera d) ha l'obbligo di conservare direttamente e specificatamente gli estremi identificativi delle persone fisiche preposte quali amministratori di base dati.

Nomina dell'Amministratore di sistema, Amministratore di base dati, Amministratore di rete.

La nomina di uno o più Amministratore di sistema, Amministratore di base dati, Amministratore di rete deve essere effettuata dal Titolare con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata per accettazione.
Copia di tale nomina accettata deve essere conservata a cura del titolare del trattamento in luogo sicuro.
Il titolare del trattamento deve informare ciascun Amministratore di sistema, Amministratore di base dati e Amministratore di rete, delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal Codice in materia di protezione dei dati personali e del disciplinare tecnico in materia di misure di sicurezza (allegato B al codice) e del Provvedimento del Garante del 27.11.2008.
Il titolare del trattamento deve consegnare a ciascun Amministratore di sistema, Amministratore di base dati, Amministratore di rete, una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina degli Amministratori sopra menzionati è a tempo indeterminato e decade per revoca o dimissioni dello stesso.
La nomina degli Amministratori sopra menzionata può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.
Amministratore di sistema e Amministratore di rete del Parco Adamello Brenta è la ditta PC COPY con sede in Tione di Trento, Via Pinzolo, n. 52/54 identificato nelle persone fisiche dei Signori Dorna Stefano, Dalfior Samuel e Pasotto Corrado (nominati con lettera prot. n. 1346/I/14/3 di data 24 marzo 2009).
L'Amministratore di Base di Dati è il Signor Periotto rag. Flavio (nominato con lettera prot. n. 6207/I/14/3 di data 11 dicembre 2009).

3) ANALISI RISCHI E MISURE DI SICUREZZA RELATIVE ALLE OPERAZIONI E COLLEGAMENTI EFFETTUATI

3.1. Uffici sede

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
Operazioni di trattamento dati con collegamento in rete tra il computer server e gli altri elaboratori degli uffici amministrativi. La rete funziona a circuito chiuso realizzato mediante allacciamento diretto via cavo	Quando gli elaboratori vengono utilizzati collegati in rete interna non vi è nessuna connessione con l'esterno per cui non esiste il rischio di accesso non autorizzato.	Nessuna durante l'utilizzo della rete interna.
	Possibilità che possa essere attivato da parte delle ditta esterna un collegamento illecito agli archivi contenenti i dati personali degli utenti	Per evitare tale rischio, che peraltro è conseguente solo alla attuazione di azioni illecite, occorre che l'impiegato che richiede l'aggiornamento del programma da remoto controlli, passo a passo, i collegamenti che sono effettuati dalla ditta esterna verificando che l'accesso sia limitato esclusivamente alle tabelle gestionali o al programma.
	Intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale che eventualmente siano presenti negli strumenti informatici della ditta esterna che si collega al server.	Utilizzo di programma "antivirus" aggiornato attivato in modalità "auto protezione" + scansione antivirus pianificata settimanalmente.
	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento	Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Verificare periodicamente manualmente che non siano presenti nel sistema programmi "TSR" quali ad esempio "Key Logger'97" oppure "wsock spy" che non vengono identificati dalla protezione antivirus.
	Violazione e modifica della integrità dei dati con programmi contenenti virus informatici	Utilizzo programma "antivirus" aggiornato attivato in modalità "auto protezione" " + scansione antivirus pianificata giornalmente. Non effettuare collegamenti altri collegamenti alla rete internet al di fuori di quelli autorizzati. Effettuare controlli periodici (ogni quindici giorni) a campione per verificare l'integrità dei dati archiviati. Cancellare, dopo il definitivo utilizzo, i files di testo che contengano dati sensibili. Effettuare salvataggi periodici dei dati archiviati.

Collegamento via Internet al sito Internet della Società produttrice per effettuare l'aggiornamento del programma antivirus. Ricerche via Internet e connessioni a siti per attività istituzionale dell'ente e di ricerca dati. Collegamento alle caselle di posta elettronica per la gestione della E-mail	Intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale che eventualmente siano presenti negli strumenti informatici della ditta esterna cui ci si collega per scaricare gli aggiornamenti del programma antivirus	Utilizzo di programma antivirus aggiornato attivato in modalità "auto protezione" + scansione antivirus pianificata all'accesso
	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento	Limitare il collegamento all'esterno solo ed esclusivamente al tempo necessario per aggiornare il programma antivirus e per collegamenti ad internet autorizzati e per l'utilizzo della posta elettronica. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Verificare periodicamente manualmente che non siano presenti nel sistema programmi "TSR" quali ad esempio "Key Logger'97" oppure "wsock spy" che non vengono identificati dalla protezione antivirus.
	Violazione e modifica della integrità dei dati	Utilizzo di programma "antivirus" aggiornato attivato in modalità "auto protezione" + scansione antivirus pianificata all'accesso al sistema. Non effettuare altri collegamenti alla rete internet al di fuori di quelli autorizzati. Effettuare controlli periodici a campione per verificare l'integrità dei dati archiviati. Effettuare salvataggi periodici dei dati archiviati con conservazione del supporto di back-up in un contenitore ad isolamento termico e magnetico in luogo differente da dove è collocato il computer

AREE E LOCALI	Valutazione dei rischi	Misure di protezione e sicurezza
UFFICI AMMINISTRATIVI	Intrusione illecita di terzi non autorizzati nei locali dove sono installati i computer	Gli elaboratori sono installati all'interno di ogni ufficio dell'ente dove possono accedere e sono autorizzati ad essere presenti durante l'orario di lavoro gli incaricati del trattamento dei vari uffici. L'ingresso negli uffici da parte di altre persone è autorizzato dagli addetti stessi i quali possono effettuare vigilanza contro il rischio di ingresso di persone non autorizzate. L'accesso agli elaboratori inoltre avviene solo tramite password personale di accensione come pure l'accesso alla rete. E' inoltre prevista anche la password sullo screen saver che viene attivata automaticamente durante le soste della attività lavorativa. Di giorno, al di fuori dell'orario di lavoro, la sede viene chiusa a chiave.
	Incendio-allagamento	Nell'ufficio esiste un sistema di rilevazione incendio collegato alla centralina installata nel locale portineria con allarme acustico in grado di attivare il piano di "emergenza incendi". I dati personali vengono salvati su nastro e conservati in luoghi differenti dal server. Per il pericolo di allagamento installare i computer in posizione rialzata da terra.
	Mancanza energia elettrica	Tutti i computer sono collegati al gruppo di continuità per assicurare l'erogazione dell'energia elettrica.

3.2. Analisi dei rischi

Rischi		Si/No	Descrizione dell'impatto sulla sicurezza (gravità alta/media/bassa)
Comportamenti degli operatori	Sottrazione di credenziali di autenticazione	si	bassa
	Carenza di consapevolezza, disattenzione o incuria	si	bassa
	Comportamenti sleali o fraudolenti	si	alta
	Errore materiale	si	medio
	Altro evento	si	bassa
eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno	si	bassa
	Spamming o tecniche di sabotaggio	si	bassa
	Malfunzionamento indisponibilità o degrado degli strumenti	si	bassa
	Accessi esterni non autorizzati	si	bassa
	Intercettazione di informazioni in rete	no	=====
	Altro evento	si	bassa
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	si	media
	Sottrazione di strumenti contenenti dati	no	=====
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	si	media
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	si	bassa
	Errori umani nella gestione della sicurezza fisica	si	bassa
	Altro evento	no	bassa

3.3. Misure di sicurezza adottate o da adottare

Misure	Descrizione rischi	Trattamenti interessati	Misure già in essere	Misure da adottare	Struttura o persone addette all'adozione
Password	Sottrazione e manomissione	Tutti	Password secretata		Ogni dipendente è responsabile della propria password
Antivirus	Virus su pc	Tutti	Antivirus – firewall	Aggiornamento Antivirus – firewall hardware	Amministratore di sistema
Chiusura armadi contenenti nastri backup	Sottrazione e manomissione nastri	Tutti	Chiusura armadi		Flavio Periotto
Chiusura armadi contenenti dati cartacei	Consultazione e sottrazione da parte di persone non autorizzate	Tutti	Chiusura armadi		Carmen Caola

4) ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

4.1. Manutenzione dei sistemi di elaborazione dei dati

Il Titolare (o se è designato l'Amministratore di sistema), anche avvalendosi di consulenti interni o esterni, deve verificare ogni anno:

- la situazione delle apparecchiature hardware installate con cui vengono trattati i dati;
- la situazione delle apparecchiature periferiche;
- la situazione dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- la sicurezza dei dati trattati;
- il rischio di distruzione o di perdita.

4.2. Manutenzione dei sistemi operativi e dei software installati

Il rischio di accesso non autorizzato o non consentito.

Al Titolare (o se è designato l'Amministratore di sistema) è affidato il compito di verificare ogni anno, la situazione dei sistemi operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei sistemi operativi e delle applicazioni software, per quanto riguarda:

- la sicurezza dei dati trattati;
- il rischio di distruzione o di perdita;
- il rischio di accesso non autorizzato o non consentito.

5) MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI

Il Titolare o l'Amministratore di sistema al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.
I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
Per ogni banca di dati deve predisporre le istruzioni di copia, verifica e ripristino dei dati.
In particolare per ogni banca di dati debbono essere definite le seguenti specifiche:

- il tipo di supporto da utilizzare per le copie di sicurezza dei dati;
- il numero di copie di sicurezza dei dati effettuate ogni volta;
- se i supporti utilizzati per le copie di sicurezza dei dati sono riutilizzati e in questo caso con quale periodicità;
- se per effettuare le copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate;
- le modalità di controllo delle copie di sicurezza dei dati;
- la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- il nome dell'incaricato a cui è stato assegnato il compito di effettuare le copie di sicurezza dei dati;
- le istruzioni e i comandi necessari per effettuare le copie di sicurezza dei dati;
- le istruzioni e i comandi necessari per effettuare il ripristino delle copie di sicurezza dei dati.

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato, di effettuare periodicamente la copie di sicurezza delle banche di dati trattate, in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica.

6) MISURE DA ADOTTARE PER LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITÀ

6.1. Misure generali

In considerazione di quanto disposto dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (D.lgs. n. 196 del 30 giugno 2003) e dal CODICE IN MATERIA DI DATI PERSONALI, è fatto divieto per chiunque di:

- effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile del Trattamento dei dati di dati oggetto del trattamento;
- effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del Trattamento dei dati di stampe, tabulati, elenchi, rubriche e di altro materiale riguardante i dati oggetto del trattamento;
- sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del Trattamento dei dati di stampe, tabulati, elenchi, rubriche e di altro materiale riguardante i dati oggetto del trattamento;
- consegnare a persone non autorizzate dal Responsabile del Trattamento dei dati stampe, tabulati, elenchi, rubriche e di altro materiale riguardante i dati oggetto del trattamento.

6.2. Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Al Responsabile della sicurezza e del Trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, e di nominare per ciascun ufficio un incaricato con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

6.3. Sedi

Il Parco Adamello Brenta ha la propria sede a Strembo in via Nazionale, 24, ove sono ubicati i seguenti uffici:

- Direttore
- Uffici Amministrativi
- Uffici Tecnici;
- Uffici Ambientali;
- Ufficio Comunicazione;
- Ufficio Ragioneria
- Uffici Tesiti, collaboratori, ecc
- Uffici guardaparco.

Il Parco ha poi alcuni centri visitatori situati a Daone, Spormaggiore, Mavignola, Tovel, Stenico, "Villa Santi" in C.C. Montagne e "Casa Grandi" nel comune di Tuenno, dove pur essendoci dei personal computer non vengono trattati dati sensibili.

L'edificio dove è ubicata la sede del Parco Naturale Adamello Brenta è provvista di sistema antincendio a norma di legge.

6.4. Sistemi di elaborazione

Al Titolare/al Responsabile della sicurezza e del trattamento dati è affidato il compito di redigere e di aggiornare ad ogni variazione, l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

Il Titolare/Responsabile ha il compito di assegnare le credenziali di autenticazione e di aggiornare l'elenco del personale autorizzato al trattamento dei dati con l'obbligo di verificare entro il 31 dicembre di ogni anno le

credenziali di autenticazione e di aggiornare l'elenco dei soggetti autorizzati al trattamento dei dati.
L'ente parco è dotato di un sistema informatico windows server 2003, integrato con windows server 2008 ed è in corso l'aggiornamento di tutti i server a windows server 2008. Si precisa inoltre che gli utenti in rete sono n. 86 (di cui n. 67 persone fisiche e n. 19 utenti di servizio). Gli Uffici periferici di Spormaggiore sono collegati in VPN al server del Parco e gli utenti possono lavorare in terminal-server direttamente presso la sede. Gli altri personal computer presso le "Case del Parco" sono n. 7, questi ultimi non sono collegati in rete con la sede ma comunque sono al servizio dell'Amministrazione dell'Ente.
Presso gli uffici della sede vengono effettuate operazioni di trattamento dati con collegamento in rete tra il computer server e gli altri elaboratori degli uffici. La rete funziona a circuito chiuso realizzato mediante allacciamento diretto via cavo ed inoltre ci si può collegare alla stessa rete attraverso una rete wifi protetta da password con caratteristica massima di sicurezza.

6.5. Protezione aree e locali interessati

Le macchine server sono collocate in apposito locale (sala server) dotata di:

- adeguato impianto antincendio;
- adeguato impianto di condizionamento dell'aria, revisionato in data 24 maggio 2012;
- implementazione impianto con centralina Brahms, che permette la comunicazione con l'Amministratore di Base Dati per tutti gli alert relativi a mancanza di corrente, temperature troppo elevate, ecc.;
- impianto elettrico a norma;
- gruppo di continuità.

Alla sala server accedono solamente le persone autorizzate. In assenza di tali persone e dopo la chiusura degli uffici la sala server viene chiusa.
I supporti di backup sono tenuti in appositi armadi chiusi a chiave in un locale diverso dalla sala server. Le chiavi sono date in consegna alle persone autorizzate all'accesso alla sala server.
Persone autorizzata all'accesso sono rag. Flavio Periotto, ing. Massimo Corradi, dott. Matteo Viviani e geom. Federico Cereghini, dipendenti dell'Ente, l'Amministratore di Sistema ed i tecnici accompagnati.
Al Responsabile/Titolare è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati e di nominare un incaricato con il compito di controllare direttamente i sistemi, le apparecchiature ed eventuali registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
Nel corso dell'anno 2014 si provvederà a spostare le apparecchiature del server in apposito locale ricavato nel seminterrato della sede di Strembo. Questo comporterà non solamente un risparmio del consumo di energia elettrica ma anche una maggior sicurezza nel mantenimento dei dati in quanto il locale è più ampio e con minor rischio al surriscaldamento delle apparecchiature.

6.6. Elenco degli archivi dei dati oggetto del trattamento

Al Titolare e al Responsabile della sicurezza e del Trattamento dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.
Ogni banca dati o archivio deve essere classificato in relazione alle informazioni contenute indicando se si tratta di:

- Dati personali comuni
- Dati personali sensibili
- Dati personali giudiziari.

Le banche dati in possesso del Parco Adamello Brenta vengono evidenziate nella seguente tabella:

Descrizione sintetica del trattamento		Natura dei dati trattati	Struttura di riferimento	Altre Strutture (anche esterne che concorrono al trattamento)	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S G			
Buste paga, dati del personale (economici) organi istituzionali (giunta, presidente, comitato) Collaboratori esterni, borsisti	Dipendenti, amministratori, borsisti, collaboratori esterni	X X	Ufficio personale	Ufficio ragioneria	Pc e cartaceo
Dati del personale (giuridici, ferie, permessi) corrispondenza in entrata ed in uscita, dati giudiziari dei verbali emessi dai guardaparco	Personale, cittadini diversi, amministratori, Enti publici,	X X	Ufficio protocollo	Ufficio personale Ufficio ragioneria Ufficio segreteria	Pc e cartaceo
Mandati di pagamento, atti amministrativi (convenzioni, determinazioni, delibere, contratti)	Dipendenti, amministratori, fornitori, clienti, cittadini diversi, collaboratori esterni, tesisti	X X	Ufficio ragioneria	Ufficio personale, ufficio protocollo, ufficio comunicazione, ufficio tecnico, ufficio guardaparco, ufficio fauna, ufficio didattica, ufficio tecnico-ambientale	Pc e cartaceo
Indirizzi relativi all'ente (abbonati notiziario, amministratori, dipendenti, ecc..) , timbrature del personale, dati giudiziari dei verbali emessi dai guardaparco, magazzino	Cittadini diversi, amministratori, dipendenti, tesisti, borsisti, abbonati, cittadini diversi	X X	Ufficio segreteria	Ufficio personale, ufficio protocollo, ufficio comunicazione, ufficio tecnico, ufficio guardaparco, ufficio fauna, ufficio didattica , ufficio tecnico-ambientale	Pc e cartaceo
Pratiche gare di appalto, manutenzione del personale dal punto di vista organizzativo (preparazione schede operative	Appaltatori, fornitori, dipendenti, enti pubblici	X X	Ufficio tecnico	Ufficio personale, ufficio ragioneria,	Pc e cartaceo

per predisporre buste paga, ad esempio malattie degli operai) gestione operai e piano del parco (ricostruzioni, gestione rapporti con enti proprietari)				ufficio protocollo, ufficio segreteria	
Analisi statistiche, segnaletica esterna al parco, gadget, dati relativi al concorso fotografico,	Cittadini diversi		Ufficio comunicazione		Pc e cartaceo
Progetto di educazione ambientale per le scuole	Scuole e insegnanti		Ufficio Didattica	Ufficio Segreteria	Pc e cartaceo Nb: i dati e gli indirizzi per ora sono su cartaceo, in previsione mailing list a insegnanti e scuole
Turismo sostenibile e economia sul territorio (rapporti con enti ed aziende	Amministratori vari, aziende economiche esistenti nei comuni del parco, enti pubblici ricadenti sul territorio del parco		Ufficio Carta Europea del turismo sostenibile	Ufficio Segreteria	Pc e cartaceo
Certificazione e gestione ambientale del parco, pubblicazioni, aspetto gestionale progetto mobilità , rapporti con collaboratori e professionisti per questo ambito, progetto qualità parco (gestione hotel che hanno aderito al progetto), didattica	Collaboratori, professionisti, albergatori, cittadini diversi		Ufficio tecnico-ambientale	Ufficio segreteria, ufficio protocollo	Pc e cartaceo
Aspetto preventivo e di controllo divisi per territorio su turni (database dello storico con multe e rilievi della non conformità per i progetti di certificazione. Verbali infrazioni diverse (accesso a SIATEL database per verificare i dati delle persone attraverso il numero di targa)	Cittadini diversi Enti pubblici	X	Guardaparco	Ufficio segreteria, ufficio protocollo Ufficio Forestale della Provincia Autonoma di Trento. Uffici Giudiziari	Pc e cartaceo

Le banche dati tenute in forma cartacea contenenti dati sensibili e dati giudiziari vengono conservate sia in armadi che in schedari muniti di serratura. Le banche dati tenute in forma elettronica contenenti dati sensibili e giudiziari vengono gestite in modo autonomo dal personale incaricato utilizzando adeguate misure di sicurezza concordate con il titolare e responsabile del trattamento dati, con l'amministratore di sistema e con il custode delle copie di sicurezza utilizzando, se necessario, mezzi di cifratura.

6.7. Trattamenti con l'ausilio di strumenti elettronici

6.7.1. Sistema di autenticazione informatica

Nel caso in cui il trattamento di dati personali è effettuato con strumenti elettronici, il Responsabile del trattamento deve assicurarsi che il trattamento sia consentito solamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione a uno specifico trattamento o a un insieme di trattamenti.
Deve inoltre assicurare che il trattamento di dati personali, effettuato con strumenti elettronici, sia consentito solamente agli incaricati dotati di una o più credenziali di autenticazione tra le seguenti:

- un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo;
- un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave;
- una caratteristica biometria dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Deve assicurarsi che il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi e che le credenziali di autenticazione non utilizzate da almeno sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Deve inoltre assicurarsi che le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
Ad ogni Incaricato del trattamento possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.
La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al numero massimo consentito.
La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La parola chiave deve essere modificata dall'incaricato del trattamento al primo utilizzo, e successivamente, almeno ogni sei mesi.
In caso di trattamento di dati sensibili o di dati giudiziari la parola chiave deve essere sostituita almeno ogni tre mesi.
Gli incaricati debbono adottare le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc…).
In particolare è fatto divieto comunicare a chiunque altro le proprie credenziali di accesso al sistema informatico.
Gli incaricati hanno l'obbligo di:

- non lasciare incustodito il proprio posto di lavoro;
- chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.

L'Incaricato della custodia delle copie delle credenziali ha il compito di assicurare la disponibilità dei dati e degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
La custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza.
L'Incaricato della custodia delle copie delle credenziali deve informare tempestivamente l'Incaricato del trattamento ogni qualvolta sia stato effettuato un tale tipo di intervento.

6.7.2. Sistema di autorizzazione

Il Responsabile della sicurezza e del trattamento ha il compito di individuare gli Incaricati del trattamento per ogni tipologia di banca di dati personali trattata.
Il tipo di trattamento effettuato da ogni singolo Incaricato del trattamento può essere differenziato.
In particolare ad ogni Incaricato del trattamento può essere data dal Responsabile del trattamento la possibilità di:

- inserire nuove informazioni nella banca di dati personali;
- accedere alle informazioni in visualizzazione e stampa;
- modificare le informazioni esistenti nella banca di dati personali;
- cancellare le informazioni esistenti nella banca di dati personali.

6.8. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

Il Responsabile della sicurezza e del trattamento dei dati ha il compito di assegnare le credenziali di autenticazione e di aggiornare l'elenco personale autorizzato al trattamento dei dati personali.
Il Responsabile del trattamento dei dati ha il compito di verificare ogni anno entro il 31 dicembre, le credenziali di autenticazione e di aggiornare l'elenco dei soggetti autorizzati al trattamento.
I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

6.9. Formazione degli incaricati del trattamento

Il Responsabile della sicurezza e del trattamento dei dati valuta, per ogni incaricato a cui ha affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione.
La previsione di interventi formativi degli incaricati del trattamento, ha lo scopo principale di renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.
La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansione, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali.
Si ritiene necessario effettuare momenti di formazione ogni qualvolta il responsabile del trattamento ne ravvisi la necessità.

6.10. Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

Il Responsabile del trattamento dei dati può decidere, sentito il titolare, di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
Deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indicare per ognuno di essi il tipo di trattamento effettuato, specificando:

- i soggetti interessati;
- i luoghi dove fisicamente avviene il trattamento di dati personali;
- i responsabili del trattamento di dati personali.

Nel caso in cui, per trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, i responsabili del trattamento di dati personali non vengano

espressamente nominati Titolari del trattamento di dati personali affidati all'esterno della struttura del titolare ovvero Titolari in Out-sourcing, ai sensi dell'art. 28 del CODICE IN MATERIA DI DATI PERSONALI, devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.
Il Responsabile del trattamento dei dati, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti individuati all'art. 29 del CODICE IN MATERIA DI DATI PERSONALI (esperienza, capacità ed affidabilità).
Il Titolare a cui è stato affidato il trattamento dei dati all'esterno deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.
Il Parco Naturale Adamello Brenta ha affidato all'esterno diversi trattamenti di dati, come si può evidenziare nella tabella seguente
NB: I dati vengono così codificati:

- dati comuni 1
- dati sensibili 2
- dati giudiziari 3

Descrizione sintetica dell'attività esternalizzata	Trattamento di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Contabilità varia	Contabilità dell'ente – gestione fornitori	Informatica Trentina spa	Designato da direttore
Gestione paghe	Stipendi, emolumenti, trattenute personale dipendente	Cba di Rovereto	Designato da direttore
Tenuta contabilità	Registrazioni corrispettivi, fatture emesse e di acquisto. Tenuta contabilità I.V.A., stesura dichiarazione I.C.I., modello unico e modello 770	Studio Associato Antolini e Studio Paoli entrambi di Tione di Trento	Designato da direttore
Igiene e sicurezza del lavoro	Visite mediche D.lgs 81/2008 e ss.mm. ed integrazioni	Cogesil	Designato da direttore

6.11. Nomina del titolare del trattamento in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Responsabile del trattamento dei dati deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.
Deve informare il Titolare del trattamento personali affidati all'esterno della struttura del titolare ovvero il Titolare in Out-sourcing, dei compiti che gli sono assegnati in relazione alle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.
La nomina del Titolare del trattamento personali affidati all'esterno della struttura del titolare ovvero il Titolare in Out-sourcing deve essere controfirmata per accettazione e copia della lettera di nomina deve essere conservata a cura del responsabile del trattamento dei dati in luogo sicuro.

6.12. Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

6.12.1. Protezione contro l'accesso abusivo

Al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, il Responsabile del trattamento dei dati, stabilisce, con il supporto del Titolare o dell'Amministratore di sistema, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.
I criteri debbono essere definiti dal Responsabile del trattamento dei dati in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- le misure applicate per evitare intrusioni;
- le misure applicate per evitare contagi da Virus informatici.

6.12.2. Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Il Responsabile del trattamento dei dati è responsabile della custodia e della conservazione dei supporti utilizzati per le copie dei dati.
Per ogni banca di dati deve essere individuato il luogo di conservazione copie dei dati in modo che sia convenientemente protetto dai potenziali rischi di:

a) Agenti chimici
b) Fonti di calore
c) Campi magnetici
d) Intrusione e atti vandalici
e) Incendio
f) Allagamento
g) Furto.

L'accesso ai supporti utilizzati per le copie dei dati è limitato per ogni banca di dati a:

- Incaricato delle copie di sicurezza delle banche dati
- Responsabile del trattamento dei dati.

6.12.3. Riutilizzo dei supporti rimovibili

Se il Responsabile del trattamento dei dati decide che i supporti magnetici contenenti dati sensibili o giudiziari non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.
Deve assicurarsi che in nessun caso vengano lasciate copie di banche di dati contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

6.12.4. Ripristino dell'accesso ai dati in caso di danneggiamento

La decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del Responsabile del trattamento dati.
La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro 7 giorni.

Una volta valutata l'assoluta necessità di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento il Responsabile del trattamento dei dati deve provvedere tramite l'Incaricato delle copie di sicurezza delle banche dati all'operazione di ripristino dei dati.
La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti deve essere presa rapidamente e in ogni caso la funzionalità deve essere ripristinata al massimo entro sette giorni.

6.12.5. Misure di tutela e di garanzia

Nel caso in cui ci si avvale di soggetti esterni alla propria struttura, per provvedere al controllo del buon funzionamento hardware e/o software degli strumenti elettronici e alla eventuali riparazione, aggiornamento o sostituzione, il Responsabile del trattamento dei dati, deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta con la descrizione dettagliata delle operazioni eseguite che attesti la conformità a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (D.lgs. n. 196 del 30 giugno 2003), con particolare riferimento a quanto stabilito al punto 25 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME SICUREZZA (Allegato B).

6.13. Trattamenti senza l'ausilio di strumenti elettronici

Per ogni archivio il Responsabile del trattamento dati deve definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso negli archivi.
Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.
Qualora i documenti contengano dati sensibili o giudiziari ai sensi dell'art. 4 del CODICE IN MATERIA DI DATI PERSONALI, gli incaricati del trattamento sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.
L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

6.13.1. Copie degli atti e dei documenti

In base a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (D.lgs. n. 196 del 30 giugno 2003) e dal DISCIPLINALRE IN MATERIA DI MISURE MINIME DI SICUREZZA, è fatto divieto a chiunque di:

- effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del Trattamento dei dati di stampe, tabulati, elenchi, rubriche e di altro materiale riguardante i dati oggetto del trattamento;
- sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del Trattamento dei dati di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- consegnare a persone non autorizzate dal Responsabile del Trattamento dei dati stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

L'Ente si è dotato inoltre di n. 3 Distruggi documenti.

7) ELENCO INCARICATI AL TRATTAMENTO DATI

Adolfo Artini (Villa Santi)
Alberto Aprili
Alessandro Ghezzo
Alessia Scalfi
Andrea Alfredo Mustoni
Anna Salmi
Antonella Diprè
Antonello Zulberti
Antonio Caola (Presidente)
Bruno Battocchi
Carmen Caola
Catia Hvala
Chiara Scalfi
Chiara Grassi
Denise Bressan
Eileen Zeni
Elisa Cattani
Enrico Dorigatti
Enrico Noro
Enrico Povinelli
Federica Castellani
Federico Cereghini
Fernando Ballardini
Filippo Zibordi
Flavio Periotto
Gilberto Volcan
Giovanni Luigi Maffei
Giuliana Pincelli
Giuseppe Alberti
Iginio Giuliani
Ilaria Rigatti
Iris Mosca
Lara Beltrami
Laura Andreolli
Laura Nave
Lina Buratti
Lorenzo Mosca
Luciano Ramponi
Luigina Armani
Manuela Gottardi
Marco Armanini
Maria Cavedon
Maria Scalfi
Martina Tomasi
Marzia Pin
Massimo Corradi
Matteo Viviani
Matteo Zeni
Michele Ruppert
Michele Zeni
Paola Albertini
Paola Franchini

Pino Oss Cazzador
Rita Onestinghel
Roberto Zoanetti
Rudy Cozzini
Valentina Beltrami
Valentina Cunaccia
Vigilio Bonazza
Violette Masè.

I N D I C E

Parte integrante e sostanziale della deliberazione della Giunta esecutiva n. 22 di data 24 marzo 2014.

Il Segretario
f.to dott. Roberto Zoanetti

Il Presidente
f.to Antonio Caola