Aree Protette
Appennino Piemontese

Regione Piemonte
Ente di gestione delle Aree protette dell'Appennino Piemontese
Bosio, Alessandria

VERBALE DI DELIBERAZIONE DEL CONSIGLIO N. 8/2020
Seduta straordinaria

OGGETTO: GDPR n. 679/2016 - approvazione procedura per la gestione della violazione dei dati personali (data breach).

L'anno duemilaventi, addì 11 febbraio, alle ore 21.20, presso la sede amministrativa dell'Ente di gestione in via Umberto I n. 32/A, Bosio (AL), sono stati per oggi convocati i componenti di questo Consiglio. All'appello risultano:

N. d'ordine	Cognome e Nome		Presenti	Assenti
1	Danilo Repetto	Presidente	X	
2	Marco Guerrini	Vice Presidente	X	
3	Francesco Giovanni Arecco	Consigliere	X	
4	Giacomo Briata	Consigliere	X	
5	Marco Moro	Consigliere	X	
		TOTALI	5	/

Visto il D.P.G.R. n. 77 del 30 dicembre 2019 "XI Legislatura. Nomina del Presidente e dei componenti del Consiglio dell'Ente di gestione delle Aree protette dell'Appennino piemontese ai sensi della legge regionale 19 giugno 2009, n. 19 e s.m.i. (Testo unico sulla tutela delle aree naturali e della biodiversità)".

Assiste all'adunanza con funzioni di Segretario verbalizzante il dott. Andrea De Giovanni, Direttore dell'Ente di gestione, il quale provvede alla redazione del presente verbale.

Il sig. Danilo Repetto, nella sua qualità di Presidente, constatata la presenza del numero legale per la validità della seduta, dichiara aperta la seduta e pone in discussione quanto in oggetto.

IL CONSIGLIO

Udita la relazione del Presidente.

Vista la L.R. n. 19/2009 e s.m.i. “Testo unico sulla tutela delle aree naturali e della biodiversità”.

Visto lo Statuto dell’Ente di gestione del Parco naturale delle Capanne di Marcarolo approvato con D.P.G.R. n. 1 del 8/1/2014.

Visto lo Statuto dell’Ente di gestione delle Aree protette dell’Appennino piemontese adottato con D.C. n. 31 del 9 agosto 2017.

Premesso che:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che 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;
- l’Ente di gestione delle Aree protette dell’Appennino Piemontese, in quanto Titolare del trattamento, è tenuto a mantenere sicuri i dati personali trattati nell’ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (data breach), incluse eventuali notifiche all’Autorità di controllo competente ed eventuali comunicazioni agli interessati.

Presa visione:

- del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 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, di seguito “Regolamento”);
- del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» (di seguito “Codice”);
- del decreto legislativo 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito “d.lgs. n. 51/2018”);
- delle “Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679” (WP250) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018;
- della Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adottata ai sensi dell’art. 64 del Regolamento, dal Comitato europeo per la protezione dei dati in data 12 marzo 2019;
- del Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [doc-web n. 9126951].

Considerato che in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal

momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del Regolamento, art. 2-bis del Codice).

Considerato inoltre che il titolare del trattamento è tenuto altresì a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero (artt. 26 e 37, comma 6, del d.lgs. n. 51/2018).

Dato atto che:

- per «violazione dei dati personali» (data breach) si intende la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del d.lgs. n. 51/2018);
- per la omessa notifica di data breach all'Autorità di controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative (art. 83 GDPR), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile);
- lo stesso GDPR, all'art. 83 paragrafo 2, indica dei fattori che possono mitigare o aggravare la violazione e, tra questi, un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del titolare che possa dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione. L'atteggiamento reattivo e cooperativo comporta, inoltre, sicuramente un'attenuazione delle sanzioni applicabili.

Ritenuto pertanto:

a) di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (data breach policy). A tale riguardo si precisa che, presso il Titolare, sono già state attivate procedure a tutela della sicurezza dei dati, tra cui:
    - l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;
    - l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi;
    - la predisposizione di un sistema di protezione, mediante apposite misure tecniche (firewall, antivirus,…) dell'accesso a internet e ai dispositivi elettronici;

b) strategico per l'ente:

- sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);

- definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
- assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate;
- stabilire che le procedure contemplate nell'approvando documento siano applicabili a tutte le attività svolte dal Titolare, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni;
- stabilire che il rispetto dell'adottanda procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia. In particolare le procedure medesime sono rivolte a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare, quali:
    1) i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;
    2) qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare. In particolare, ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach.

Visto il Decreto del Presidente numero 10 del 21 maggio 2018 con il quale è stato designato l'avv. Massimo Ramello quale Responsabile della Protezione dei Dati Personali (DPO), nel rispetto della vigente normativa, nonché il F.A. Annarita Benzo (Responsabile del trattamento dei dati dell'Ente), quale soggetto interno all'Ente, con compiti di "unico" referente del DPO.

Vista la nota del 9/12/2019 (prot. APAP n. 2600/2019), allegata alla presente, pervenuta dall'Avv. Massimo Ramello in qualità di Responsabile della protezione dei dati dell'Ente, inerente la necessità di predisporre una procedura organizzativa interna.

Visto il documento "Disposizioni operative in materia di incidenti di sicurezza e di violazione di sati personali (c.d. data breach), allegato alla presente.

Ritenuto di approvate la procedura nel caso di violazione dei dati personali (data breach) dell'Ente di gestione delle Aree protette dell'Appennino Piemontese, richiesta dagli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679), allegato alla presente.

Visto che la votazione, avvenuta a norma di legge, per alzata di mano, ha dato i seguenti risultati:
Votanti: 5;
Astenuti: 0;
Favorevoli: 5;
Contrari: 0.

Dato atto che ai sensi e per gli effetti del vigente Statuto dell'Ente Parco è stato apposto il visto del

Direttore dott. Andrea De Giovanni in ordine alla regolarità amministrativa.

DELIBERA

di approvare la procedura nel caso di violazione dei dati personali (data breach) dell'Ente di gestione delle Aree Protette dell'Appennino Piemontese, richiesta dagli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679), allegata alla presente;

di trasmettere la suddetta procedura al Responsabile del Trattamento dei Dati personali già nominato, in persona dell'Avv. Massimo Ramello;

di trasmettere inoltre copia della presente deliberazione al F.A. Annarita Benzo (Responsabile del trattamento dei dati) e a tutto il personale dipendente per opportuna conoscenza, per attuazione e per quanto di competenza;

di disporre che al presente provvedimento venga assicurata:

- la pubblicità legale con pubblicazione all'Albo Pretorio;
- la massima diffusione presso tutto il personale operante presso l'Ente e presso tutti i soggetti esterni qualificabili in termini di responsabili del trattamento.

di pubblicare la presente deliberazione all'Albo Pretorio dell'Ente di gestione delle Aree protette dell'Appennino piemontese (www.areeprotetteappenninopiemontese.it), nonché nel sito istituzionale dell'Ente di gestione nella sezione "Amministrazione Trasparente" ai sensi dell'art. 23, comma 1, lett. d) del D.Lgs. n. 33/2013 e s.m.i.

Allegato 1: Data breach policy.
Allegato 2: Allegato A.
Allegato 3: Allegato B.
Allegato 4: Allegato C.
Allegato 5: Allegato D.
Allegato 6: Allegato E.

Il presente verbale viene letto, approvato e sottoscritto:

IL PRESIDENTE
Danilo Repetto

(Firmato digitalmente)

IL DIRETTORE f.f.
dott. Andrea De Giovanni

(Firmato digitalmente)

F.to in originale

****

ATTESTATO DI PUBBLICAZIONE

Si attesta che la presente Deliberazione viene pubblicata all'Albo Pretorio di questo Ente per 15 giorni consecutivi a partire dal 12/2/2020

IL FUNZIONARIO AMMINISTRATIVO
Sig.ra Annarita Benzo
(Firmato digitalmente)

In ordine alla regolarità amministrativa e contabile, ai sensi e per gli effetti del vigente Statuto dell'Ente di gestione e della D.D. n. 22/2014, è apposto il visto favorevole.

IL FUNZIONARIO AMMINISTRATIVO
Sig.ra Annarita Benzo
(Firmato digitalmente)

In ordine alla regolarità amministrativa, ai sensi e per gli effetti del vigente Statuto dell'Ente di gestione e della D.D. n. 22/2014, è apposto il visto favorevole.

IL DIRETTORE f.f.
dott. Andrea De Giovanni
(Firmato digitalmente)

F.to in originale

INVIO AL SETTORE GESTIONE AREE PROTETTE DELLA REGIONE PIEMONTE

La presente Deliberazione è stata trasmessa al Settore Biodiversità e Aree Naturali della Regione Piemonte in data_____, nostro prot. n. _____, con elenco n. _____

Bosio, lì _____

IL FUNZIONARIO AMMINISTRATIVO
Sig.ra Annarita Benzo
(Firmato digitalmente)

F.to in originale

Divenuta esecutiva in data ……

****

copia conforma all'originale
per uso amministrativo

IL DIRETTORE f.f.
dott. Andrea De Giovanni
(Firmato digitalmente)

IL FUNZIONARIO AMMINISTRATIVO
Sig.ra Annarita Benzo
(Firmato digitalmente)

Bosio, lì _____

****

Inserita Variazione/Prelievo in data _____ Firma e Timbro _____