**REGIONE PIEMONTE**
**Ente di Gestione delle**
**Aree Protette della Valle Sesia**

# VERBALE DI DELIBERAZIONE DEL CONSIGLIO DIRETTIVO

**N. 21**

**del 14/06/2023**

**OGGETTO: APPROVAZIONE DELLA PROCEDURA DELL'ENTE PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)**

L'anno duemilaventitre addì quattordici del mese di giugno alle ore 18, in modalità mista in presenza, presso la sede dell'Ente di Gestione delle Aree Protette della Valle Sesia in Corso Roma 35 - Varallo VC, e da remoto, ai sensi del Regolamento per il funzionamento delle riunioni degli organi dell'Ente di gestione delle Aree protette della Valle Sesia in modalità telematica, approvato con deliberazione del Consiglio n. 10 del 26/5/2022, previa l'osservanza di tutte le disposizioni di legge e le formalità vigenti, si è riunito, per convocazione del Presidente, il Consiglio Direttivo dell'Ente di gestione delle Aree Protette della Valle Sesia.

Assume la Presidenza il Dott. Carlo Stragiotti assistito dalla Dott.ssa Lucia Pompilio con funzioni di Segretario verbalizzante.

Il Presidente dà incarico al Segretario di procedere all'appello dei Consiglieri:

| CONSIGLIERI | PRESENTI | ASSENTI |
|---|---|---|
| STRAGIOTTI Carlo | X | |
| ANNOVAZZI Maria Teresa | X | |
| DEGASPARIS Andrea | X | |
| FERRARIS Giuseppe | X | |
| TAMBORNINO Egidio | X | |
| VAIRA Filiberto | X | |

Dei quali sono presenti n. 6.

I Consiglieri Degasparis, Ferraris, Tambornino e Vaira sono collegati da remoto mediante piattaforma zoom.

## IL CONSIGLIO

Visto l'art. 12 lettera k) della L.R. 19/2009 e s.m.i. "Testo unico sulla tutela delle aree naturali e della biodiversità", che istituisce l'Ente di gestione delle aree protette della Valle Sesia, al quale sono affidati in gestione il Parco Naturale dell'Alta Val Sesia e dell'Alta Val Strona e il Parco Naturale del Monte Fenera;

Vista la Deliberazione del Consiglio dell'Ente di gestione delle Aree protette della Valle Sesia n. 1 del 2.03.2020 di insediamento del Presidente e del Consiglio dell'Ente stesso.

Visto il Decreto del Presidente della Giunta Regionale n. 19 del 12 maggio 2023 con cui è stato nominato il Sig. Carlo Stragiotti, in sostituzione del Presidente dimissionario sig. Paolo Ferrari, al fine di consentire l'integrazione della compagine consiliare dell'Ente;

Riconosciuta la legalità della seduta, essendo presente la maggioranza assoluta dei Consiglieri in carica, ai sensi dell'art. 12 dello Statuto dell'Ente, approvato con deliberazione del Consiglio n. 7 del 7/4/2022;

Visto l'art. 14, comma 2 della L.R. n. 19/2009 e s.m.i. che individua le funzioni dei Presidenti degli Enti di gestione delle aree protette piemontesi;

Preso atto della deliberazione di Consiglio n. 1 dell'01.02.2021 di attribuzione dell'incarico di Direttore dell'Ente, ai sensi dell'art. 15 della L.R. n. 19/2009 e s.m.i., alla Dirigente Dott.ssa Lucia Pompilio;

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 della Valle Sesia, 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;

VISTO

- il 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");

- il 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");

- il 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");

- le "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;

- la 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;

- il 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);

- 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);

- 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);

- inoltre, 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:

i. 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 del prestazioni richieste per conto del Titolare del trattamento;

ii. 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;

VISTI

- la determinazione n. 46/2021 con è stato affidato l'incarico triennale alla Si.re Informatica di Novi Ligure (Al) nella persona dell'Avv. Massimo Ramello, per i servizi di Responsabile della protezione dei dati e adempimenti di cui al Regolamento UE 679/2016;

- la delibera di questo Consiglio n. 20 del 14/6/2023, con la quale è stato approvato il Modello organizzativo dell'Ente per la protezione delle persone fisiche con riguardo al trattamento dei dati personali

Con voti favorevoli unanimi espressi in forma palese,

**DELIBERA**

1. di approvare la procedura nel caso di violazione dei dati personali (data breach) dell'Ente di gestione delle Aree protette della Valle Sesia richiesta dagli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento

UE 2016/679), qui allegata quale parte integrante e sostanziale della presente deliberazione;

2. di disporre che al presente provvedimento venga assicurata la massima diffusione presso tutto il personale operante presso l'Ente e presso tutti i soggetti esterni qualificabili in termini di responsabili del trattamento.

3. di inviare la procedura nel caso di violazione dei dati personali (data breach) dell'Ente di gestione delle Aree protette della Valle Sesia al Responsabile del Trattamento dei Dati personali già nominato, in persona dell'Avv. Massimo Ramello;

4. di pubblicare la presente deliberazione all'Albo Pretorio dell'Ente di gestione delle Aree protette della Valle Sesia 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.

Letto, confermato e sottoscritto,

**Il Presidente**
Carlo Stragiotti
firmato digitalmente

**Il Segretario**
Lucia Pompilio
firmato digitalmente

Firmato digitalmente da:
POMPILIO LUCIA
Firmato il 15/06/2023 12:56
Seriale Certificato: 2396267
Valido dal 27/04/2023 al 27/04/2026
InfoCamere Qualified Electronic Signature CA

Ai sensi del D.lgs. 267/2000 art. 49 si esprime parere favorevole/non favorevole di regolarità tecnica in merito al provvedimento in oggetto.

Il responsabile

Ai sensi del D.lgs. 267/2000 art. 49 si esprime parere favorevole/non favorevole di regolarità contabile in merito al provvedimento in oggetto.

Il responsabile

La presente deliberazione è resa pubblica mediante l'Albo Pretorio digitale dell'Ente sul sito web www.areeprotettevallesesia.it

Si certifica che la presente deliberazione è stata pubblicata all'Albo Pretorio il giorno…… e vi rimane per giorni 15.

Il direttore

Avverso la presente deliberazione è ammesso ricorso entro il termine di 60 giorni innanzi alle sedi di Giurisdizione Amministrativa.

Copia conforme all'originale in carta libera ad uso amministrativa.

Lì

Il Direttore

Firmato digitalmente da STRAGIOTTI CARLO C=IT