RISERVA NATURALE MONTE NAVEGNA E MONTE CERVIA

Direzione: DIREZIONE

Area:

DETERMINAZIONE *(con firma digitale)*

N. A00053 **del** 29/03/2023 **Proposta n.** 67 **del** 29/03/2023

Oggetto:

Regolamento UE 2016/679 procedure e linee guida da seguire in casi di Data Breach

Proponente:

Estensore	PIVA GIOVANNI	_____*firma elettronica*_____
Responsabile del procedimento	PIVA GIOVANNI	_____*firma elettronica*_____
Responsabile dell' Area		_____
Direttore	VINCENZO LODOVISI	_____*firma digitale*_____

Firma di Concerto

Richiesta di pubblicazione sul BUR: NO

IL DIRETTORE

VISTA la Legge Regionale n° 56 del 09/09/1988 istitutiva di questa Riserva Naturale;

VISTA la Legge Regionale 22 maggio 1995, n. 29, avente ad oggetto "Modifiche ed integrazioni leggi regionali in attuazione all'art. 13 della legge regionale 18 novembre 1991, n. 74 (Disposizioni in materia di tutele ambientale – Modifiche ed integrazioni alla legge regionale 11 aprile 1985, n. 36);

VISTA la Legge 6 dicembre 1991, n. 394 "Legge Quadro sulle Aree Protette";

VISTA la Legge Regionale 6 ottobre 1997, n. 29, "Norme in materia di aree naturali protette regionali" e successive modificazioni;

VISTO l'art. 9 della Legge Statutaria Regionale 11 novembre 2004, n. 1, di approvazione del "Nuovo Statuto della Regione Lazio";

VISTA altresì, la Legge Regionale14 luglio 2014 n° 7, che all'art. 1 stabilisce funzioni e compiti degli organi di controllo degli enti pubblici dipendenti della Regione Lazio;

VISTO il Decreto del Presidente della Regione Lazio n° T00018 del 15/01/2020 di nomina del Direttore della Riserva Naturale Monte Navegna e Monte Cervia nella persona del Dott. Vincenzo Lodovisi;

VISTO il contratto di diritto privato per il conferimento dell'incarico di Direttore del Parco, sottoscritto tra il Presidente e il Dott. Vincenzo Lodovisi in data 03/02/2020;
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");

VISTO 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");

VISTO 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 "Decreto");

VISTE le “Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679” adottate del Gruppo di lavoro articolo 29 per la protezione dei dati personali il 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018, fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018;

VISTO il “Parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati” adottato dal Comitato europeo per la protezione dei dati il 12 marzo 2019;

CONSIDERATO che per “violazione dei dati personali” 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 e art. 2, comma 1, lett. m), del Decreto);

RILEVATO che, in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare la violazione 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 e art. 2-bis del Codice);

RILEVATO, altresì, che il titolare del trattamento è tenuto 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 Decreto);

VISTO il provvedimento n. 157 del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951), con il quale il Garante - ritenendo eliminati e sostituiti i termini temporali, il contenuto e le modalità della comunicazione delle violazioni di dati personali ai sensi della disciplina previgente l’applicazione del Regolamento - ha indicato le informazioni che i soggetti tenuti alla notifica delle violazioni dei dati personali forniscono al Garante nell’adempimento dell’obbligo previsto dall’art. 33 del Regolamento e dall’art. 26 del Decreto, nonché le modalità con le quali effettuare la predetta notifica;

VISTO il decreto legislativo 7 marzo 2005, n. 82, recante “Codice dell'amministrazione digitale”, e, in particolare, l’art. 64-bis, comma 1-quater, che prevede, tra l’altro, che “i soggetti di cui all'articolo 2, comma 2, lettera a), rendono fruibili tutti i loro servizi anche in modalità digitale”;

CONSIDERATO che al Garante è attribuito il compito di promuovere la consapevolezza dei titolari del trattamento e dei responsabili del trattamento

riguardo agli obblighi imposti loro dal Regolamento e dal Decreto (art. 57, par. 1, lett. d), del Regolamento e art. 37, comma 2, lett. b), del Decreto);

Visto il Provvedimento del garante della privacy 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach)

Visto l'allegato documento relativo alla procedura da adottare in caso di Data Breach

DETERMINA

1) Le premesse sono parte integrante e sostanziale del presente atto e ne costituiscono motivazione

2) Di prendere atto ed approvare l'allegata procedura da adottare in caso di eventi di data breac

3) La pubblicazione del presente atto avverrà tramite affissione all'albo pretorio telematico

POLYCY DATA BREACH ai sensi dell'Articolo 33 del GDPR

FINALITA' E AMBITO DI APPLICAZIONE

fornire procedure e linee guida da seguire in casi di Data Breach secondo gli obblighi imposti dal regolamento europeo 2016/679

Destinatari

Al fine di garantire la tutela e i diritti degli interessati, la presente Policy è messa a disposizione e deve essere osservata dai seguenti soggetti:

- Titolari del trattamento
- Responsabile della Protezione Dati, ove nominato
- Incaricati al trattamento del titolare per le sole finalità e con le modalità connesse alle loro responsabilità e mansioni lavorative
- Responsabili del titolare per le sole finalità e con le modalità alle loro responsabilità e obbligazioni contrattuali

COMITATO DI CRISI

Per la gestione e la mitigazione e risoluzione di tutti gli adempimenti derivanti dal Regolamento Europeo in materia di Data Breach , il Titolare del trattamento ha individuato un comitato di crisi composto da il :

Dirigente incaricato….

Responsabile settore IT

Data Protection officer

DATA BREACH

Qualsiasi atto, volontario o involontario, interno o esterno, che comporti la distruzione, il danneggiamento, la perdita, la modifica, la rivelazione, l'accesso non autorizzato, o il trattamento illecito o senza autorizzazione di Dati Personali trasmessi, conservati o comunque elaborati dal Titolare costituisce un Data Breach.

OBBLIGHI DEL TITOLARE IN CASO DI DATA BREACH

Il Titolare del trattamento è tenuto a notificare al Garante per la Protezione dei Dati personali il Data Breach senza ritardo e cmq entro 72 ore dal momento in cui ne viene a conoscenza a meno che tale evento non costituisca un rischio per i diritti e le libertà delle persone fisiche

Il Titolare del trattamento è considerato ***consapevole*** del Data Breach a partire dal momento in cui vi sia un ragionevole grado di certezza riguardo al fatto che l'incidente si sia verificato e che i dati personali siano stati compromessi.

Inoltre, il Titolare del trattamento è considerato ***consapevole*** del Data Breach nel momento in cui ne vengono a conoscenza i Responsabili del trattamento. Pertanto, il Titolare del Trattamento deve implementare opportune misure di sicurezza tali da obbligare ciascun Responsabile del trattamento a comunicare anche il solo sospetto di occorrenza di un evento qualificabile come Data Breach.

Il Titolare del trattamento deve rendere noto a chiunque tratti, a qualsiasi titolo, i propri Dati Personali l ' obbligo di segnalare immediatamente qualsiasi Data Breach tramite casella di posta elettronica certificata .

VALUTAZIONE

A seguito della segnalazione di un Data Breach, il Titolare del trattamento è tenuto ad effettuare una valutazione circa la possibilità che da questo derivi un rischio per i diritti e le libertà degli Interessati.

Il rischio in questione esiste se dalla violazione possono derivare danni fisici, materiali o immateriali, agli interessati, quali perdita del controllo dei Dati personali, limitazione di diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei Dati Personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica. Inoltre, particolare attenzione dovrà essere posta in caso di Data Breach che coinvolga Dati Particolari o Dati relativi alla salute.

Nella valutazione, il Titolare del trattamento deve tenere conto della probabilità del rischio e della sua gravità basandosi su:

- Tipo di violazione: la gravità del rischio può essere diversa a seconda che venga violata la confidenzialità dei dati, la loro disponibilità, o l' integrità di questi.
- Tipo di dati oggetto del Data Breach: più i dati sono "sensibili"- e quindi appartenenti a categorie particolari di dati personali – più alto sarà il rischio per gli interessati.
- Facilità con la quale l'Interessato può essere identificato: in alcuni casi, infatti, a seguito di una violazione, tale attività può risultare particolarmente semplice .
- Gravità delle conseguenze per gli Interessati: a seconda della natura dei dati violati, le conseguenze possono essere particolarmente serie.
- Caratteristiche peculiari degli interessati: alcune categorie di soggetti, ad esempio i bambini, rischiano di essere maggiormente esposti in caso di violazione.
- Numero di individui Interessati: maggiore è il numero di soggetti, maggiori rischiano di essere le implicazioni di un eventuale Data Breach. Anche in questo caso, però, è necessario valutare le singole circostanze, in quanto, in alcuni casi, la violazione può comportare anche gravi rischi per il singolo.
- Eventuali caratteristiche del titolare del trattamento: anche questo è un elemento da tenere in considerazione, in quanto, a seconda del tipo di attività svolta, la violazione può essere piu o meno grave.

ESITO DELLA VALUTAZIONE E OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

La valutazione del Titolare del trattamento si conclude con una delle seguenti decisioni.

- Il Data Breach non comporta rischi per le libertà e i diritti degli interessati
- Dal Data Breach possono derivare rischi per i diritti e le libertà degli Interessati

- Il Data Breach presenta un rischio elevato per le libertà e i diritti delle persone fisiche.

NESSUN RISCHIO PER I DIRITTI E LE LIBERTA'

Qualora dalla valutazione del Titolare del trattamento sia emerso che il Data Breach non ha comportato rischi per i diritti e le libertà degli Interessati, il Titolare si limiterà ad aggiornare il Registro dei Data Breach, annotandovi puntualmente gli eventi e le conseguenze del Data Breach, i dati interessati e i provvedimenti adottati per porvi rimedio.

RISCHI PER LA LIBERTA' E I DIRITTI DEGLI INTERESSATI

Qualora dalla valutazione del Titolare del trattamento sia emerso che dal Data Breach possono derivare rischi per le liberta e i diritti degli Interessati, il Titolare del trattamento è obbligato a notificare l 'incidente all' Autorità Garante.

La notifica avverrà entro 72 ore dal momento in cui il Titolare del trattamento è venuto a conoscenza della violazione. Laddove non sia possibile rispettare le tempistiche prescritte, sarà necessario indicare i motivi del ritardo.

Se le circostanze del caso lo richiedono, il Titolare del trattamento può delegare l' attività di notifica del Data Breach al Responsabile del trattamento che sia venuto a conoscenza della violazione.

La notifica del Data Breach all' Autorità Garante dovrà contenere almeno le seguenti informazioni:

- La descrizione della natura delle violazioni dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti dal Data Breach, nonché le categorie e il numero approssimativo di registrazioni dei dati personali
- IL nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere ulteriori informazioni.
- La descrizione delle probabili conseguenze della violazione dei Dati Personali.
- La descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio al Data Breach o attenuare possibili effetti negativi.
- Ogni altra informazione utile per proteggere i diritti e le libertà degli Interessati.

Nel caso in cui entro le 72 ore dalla scoperta del Data Breach il Titolare del trattamento non sia in possesso di tutte le informazioni sopra indicate, dovrà darne esplicita comunicazione all' Autorità Garante, concordando con questa le modalità e i termini per integrare le informazioni.

RISCHIO ELEVATO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE

Qualora dalla valutazione del Titolare del trattamento sia emerso che il rischio per le libertà e i diritti delle persone fisiche è elevato, in aggiunta alla notifica al Garante il Titolare del Trattamento è obbligato a comunicare il Data Breach anche agli Interessati.

La notifica agli interessati, da effettuarsi senza ingiustificato ritardo, dovrà illustrare in maniera chiara e semplice la natura del Data Breach e contenere almeno:

- Il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni.

- La descrizione delle probabili conseguenze della violazione dei dati personali.
- La descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio al Data Breach e anche, se del caso, per attenuarne i possibili effetti negativi.
- Ulteriori informazioni ritenute di volta in volta opportune dal Titolare del trattamento.

La comunicazione dovrà essere effettuata direttamente ed individualmente agli Interessati, a meno che ciò non rappresenti uno sforzo sproporzionato. Il Titolare del trattamento potrà comunque interpellare all' Autorità Garante per ottenere indicazioni delle modalità più adeguate per la comunicazione dell'evento agli interessati.

LA COMUNICAZIONE AGLI INTERESSATI NON E' NECESSARIA SE IL TITOLARE DEL TRATTAMENTO E' IN GRADO DI DIMOSTRARE IL SODDISFACIMENTO DI ALMENO UNA DELLE SEGUENTI CONDIZIONI:

1. Il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto del Data Breach, in particolare quelle destinate a rendere i dati particolar*i incomprensibili* a chiunque non sia autorizzato ad accedervi, quali la *cifratura.*
2. Il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati.
3. La comunicazione richiederebbe sforzi sproporzionati. In tal caso, si dovrà procedere a una comunicazione pubblica o a una misura simile tramite la quale gli Interessati dovranno essere informati con analoga efficacia

DOCUMENTAZIONE DATA BREACH

Ogni azione intrapresa dal Titolare del trattamento e dal comitato di crisi dalla scoperta del Data Breach sino alla definitiva gestione va documentata.

REGISTRO DELLE VIOLAZIONI DI DATI PERSONALI

Numero progressivo	Breve descrizione evento	Tempo	Luogo	Tipo di violazione	Dispositivi interessati	Numero soggetti interessati	Dati interessati	Gravità del Data Breach	Comunicazio al garante
	Es. accesso abusivo da esterno/interno/virus/attività hackers/smarrimento e/o furto apparecchiature sottrazione dei dati	Es. data dal xx/xx/xx al xx/xx/xx oppure in corso	Es. luogo fisico furto del PC presso x/accesso abusivo al sistema informatico di x oppure accesso abusivo archivio cartaceo di x	Indicare quale conseguenza ha determinato: lettura/ cancellazione/copia/ alterazione/ furto dei dati o altro	Computer/Rete/Dispositivo mobile/ pc o smartphone/File o parte di un file strumento di backup/ Documento cartaceo Altro	Potenzialmente x persone/ numero ancora sconosciuto	Dati anagrafici/codice fiscale/ Dati di accesso e identificazione (user name e password, customer ID, altro)Dati relativi a minori, Dati personali idonei a rivelare l' origine razziale ed etnica le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico, o sindacale Dati personali idonei a rivelare lo stato di salute la vita sessuale Dati giudiziari Copia	Basso/trascurabile Medio/ Alto/ Molto alto	Indicare quando se effettuata e l eventuali cause ritardo, es. non effettuata perch violazione non rappresenta un rischio per le lib e diritti degli interessati ex art.33, primo comma GDPR

							per immagine su supporto informatico di documenti analogici/ Ancora sconosciuto Altro.		