PARCO NAZIONALE FORESTE CASENTINESI, MONTE FALTERONA, CAMPIGNA

DETERMINAZIONE N. 1089 del 28-12-2021

OGGETTO: PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI - DATA BREACH - AI SENSI DEL REGOLAMENTO UE 2016/679 - APPROVAZIONE

IL DIRETTORE

PREMESSO CHE:

- 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 RGPD, in vigore dal 24 maggio 2016, e applicabile dal 25 maggio 2018, prevede che tutti i titolari del trattamento sono tenuti ad osservare una serie di obblighi per garantire la sicurezza dei dati trattati;
- il sopracitato Regolamento pone con forza l'accento sulla "responsabilizzazione" di titolari e responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento;

CONSIDERATO CHE:
- l'art. 33 del Regolamento prevede che tutti i titolari dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque senza ingiustificato ritardo, se ritengono probabile che da tale violazione derivino dei rischi per i diritti e le libertà degli interessati;
- l'art. 34 del Regolamento prevede che se la probabilità di tale rischio è elevata si dovrà informare della violazione anche gli interessati, sempre senza ingiustificato ritardo;

RILEVATO CHE:
- la notifica all'Autorità dell'avvenuta violazione è obbligatoria solo sotto particolari circostanze, subordinata alla valutazione del rischio per gli interessati;
- il Titolare dovrà comunque documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati nonché le relative circostanze e conseguenze e i provvedimenti adottati, essendo peraltro tenuto a fornire tale documentazione su richiesta all'autorità di controllo in caso di accertamenti;

VISTO il provvedimento presidenziale n. 11 del 09/09/2021 di nomina del DPO dell'Ente;

VISTO altresì il provvedimento presidenziale n. 24 del 23/12/2021 con il quale il sottoscritto è stato nominato responsabile del trattamento dei dati personali dell'Ente;

VALUTATO CHE occorre disciplinare gli aspetti organizzativi e la procedura che definisca le modalità operative, i compiti e le responsabilità relative alla gestione delle violazioni di dati personali che potrebbero comportare un rischio per i diritti e le libertà delle persone fisiche;

ATTESO che il DPO, in collaborazione con l'Ente, ha redatto il documento "PROCEDURA DATA PROTECTION DATA BREACH E NOTIFICHE" allegato al presente atto per farne parte integrante e sostanziale all "A" nel quale sono definite le modalità operative, i compiti e le responsabilità relative alla gestione delle violazioni di dati personali, comprensivo dei seguenti allegati:

1. DATA BREACH ANALISI E VERBALE
2. REGISTRO DATA BREACH

RITENUTO tale documento meritevole di approvazione;

VISTO il parere di regolarità tecnica rilasciato dal sottoscritto Direttore dell'Ente e allegato al presente atto per farne parte integrante e sostanziale;

DETERMINA

1. di approvare, per le motivazioni in narrativa esposte che qui si intendono integralmente richiamate, il documento allegato al presente atto per farne parte integrante e sostanziale all "A" denominato "PROCEDURA DATA PROTECTION DATA BREACH E NOTIFICHE" nel quale sono definite le modalità operative, i compiti e le responsabilità relative alla gestione delle violazioni di dati personali, comprensivo dei seguenti allegati:

    - DATA BREACH ANALISI E VERBALE
    - REGISTRO DATA BREACH

2. di dare mandato agli uffici di pubblicare la procedura nell'apposita sezione privacy del sito istituzionale dell'Ente;

3. di prendere atto del parere di regolarità tecnica rilasciato dal sottoscritto Direttore dell'Ente e allegato al presente atto per farne parte integrante e sostanziale.

Il presente atto viene confermato e sottoscritto.

FIRMATO DIGITALMENTE
IL DIRETTORE
Dott. ALESSANDRO BOTTACCI

PARCO NAZIONALE FORESTE CASENTINESI, MONTE FALTERONA E CAMPIGNA

PARERE DI REGOLARITA' TECNICA

OGGETTO: **PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI - DATA BREACH - AI SENSI DEL REGOLAMENTO UE 2016/679 - APPROVAZIONE**

SERVIZIO: **SERVIZIO DIREZIONE**

PARERE DI REGOLARITA' TECNICA E CONTROLLO DI REGOLARITA' AMMINISTRATIVA

In relazione a quanto in oggetto, verificata la rispondenza della proposta in esame alle leggi e norme regolamentari vigenti, attinenti alla specifica materia si esprime parere di regolarità tecnica **Favorevole.**

Eventuali note e prescrizioni:

Pratovecchio, 23-12-2021

FIRMATO DIGITALMENTE
BOTTACCI ALESSANDRO

PARCO NAZIONALE FORESTE CASENTINESI, MONTE FALTERONA, CAMPIGNA

DETERMINAZIONE DIRIGENZIALE

N.1089 del 28-12-2021

OGGETTO: PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI - DATA BREACH - AI SENSI DEL REGOLAMENTO UE 2016/679 - APPROVAZIONE

C E R T I F I C A T O D I P U B B L I C A Z I O N E

Il sottoscritto responsabile della pubblicazione certifica che la presente determinazione viene pubblicata il giorno 28-12-2021 all'Albo Pretorio *on line* per 15 giorni consecutivi.

Pratovecchio Stia, 28-12-2021

L'INCARICATO
DANIELA FANI

Documento informatico sottoscritto con firma digitale ai sensi dell'art. 24 del DLgs 07/03/2005 n. 82 e s.m.i (CAD)., il quale sostituisce il documento cartaceo e la firma autografa. Il presente documento è conservato in originale nella banca dati del Parco Nazionale Foreste Casentinesi Monte Falterona Campigna ai sensi dell'art. 3-bis del CAD.

Sommario

1. REVISIONI

REV.	DATA	DESCRIZIONE E RIFERIMENTI
0	15.12.2021	Redazione iniziale

2. SCOPO

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni dei dati personali trattati dall'ENTE PARCO NAZIONALE DELLE FORESTE CASENTINESI, MONTE FALTERONA E CAMPIGNA in qualità di Titolare del trattamento (di seguito anche "Titolare del trattamento"). Queste procedure sono ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.

3. APPLICABILITA'

La presente procedura si applica a tutti i dati personali trattate da ENTE PARCO NAZIONALE DELLE FORESTE CASENTINESI, MONTE FALTERONA E CAMPIGNA. Questa si riferisce a: - dati personali trattati "da "e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo; - dati personali conservati o trattati a mezzo di qualsiasi altro sistema dell'Ente. Per «dato personale» si intende: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

4. RIFERIMENTI

La presente procedura è applicata in ottemperanza a quanto prescritto dal Reg. UE 2016/679.

5. TERMINI E DEFINIZIONI

Valgono le definizioni riportate nel Regolamento Europeo 2016/679.

6. RESPONSABILITA'

La responsabilità della procedura è affidata al Titolare del Trattamento e al Responsabile del Trattamento.

7. COSA È UNA VIOLAZIONE DI DATI PERSONALI

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento.
Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà/illecito (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);

- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete dell'Ente;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, dispositivo o attrezzature informatiche dell'Ente;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

La procedura si avvale del modello **MDP-DBR Data Breach** per tutti i seguenti passaggi.

8. DESTINATARI PROCEDURA DATA BREACH

Questa procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno 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 ex art. 28 GDPR o di autonomo Titolare (genericamente denominati Destinatari esterni);

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione. Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti.

In caso il Responsabile del Trattamento Esterno nominato non rispetti la procedura prevista dall'Art. 28 GDPR, ciò può comportare, se previsto, la risoluzione del contratto in essere.

9. ATTIVITA' OPERATIVA

9.1. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti quattro step:

I. ***Step 1: Identificazione e indagine preliminare –***
II. ***Step 2: Contenimento, recovery e risk assessment –***
III. ***Step 3: Eventuale notifica all'Autorità Garante –***
IV. ***Step 4: Eventuale comunicazione agli interessati –***
V. ***Step 5: Documentazione della violazione***

Step 1: Identificazione e indagine preliminare

Nel caso in cui un dipendente si accorga o venga messo a conoscenza di una concreta o potenziale o sospetta violazione che interessa dati personali di qualsiasi natura essi siano (dati informatici o non informatici su archivi o supporti elettronici o cartacei), dovrà immediatamente comunicarla tramite e-mail al Responsabile del Trattamento

A Questo punto il dipendente, se del caso, si impegnerà ad assistere il Responsabile alla compilazione del modello ***DBR- ANALISI E VERBALE***

Il Modello ***DBR-ANALISI E VERBALE***, debitamente compilato, permetterà al Titolare del trattamento e al Responsabile, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento del DPO. Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Responsabile del Trattamento, su direttive del Titolare, dovrà coinvolgere in tutta la procedura indicata nel presente documento anche l'Amministratore di Sistema Esterno dell'Ente.

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nel modello DBR-ANALISI E VERBALE, quali:

- la data di scoperta della violazione (tempestività);
- il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già realizzate

Step 2: Contenimento, Recovery e Valutazione del Rischio

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o il Responsabile del Trattamento insieme al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati;
- isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Il Data Protection Officer, arrivato nella struttura di riferimento, monitora e controlla il regolare andamento della valutazione del Data Breach al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, tenendo conto della Valutazione della violazione e del file compilato **DBR-ANALISI E VERBALE**, nonché, dei principi e le indicazioni di cui all'art. 33 GDPR. Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Step 3: Eventuale notifica all'Autorità Garante competente

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Ente Parco Nazionale delle Foreste Casentinesi, Monte Falterona e Campigna dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza. Pertanto, il Titolare del trattamento e il DPO individueranno l'Autorità di Controllo competente sulla base delle informative e/o della valutazione d'impatto sulla protezione dei dati già in essere presso l'Ente Parco Nazionale delle Foreste Casentinesi, Monte Falterona e Campigna in relazione ai dati oggetto di violazione (in mancanza di tale documentazione che abbia preventivamente individuato l'Autorità Garante competente, la stessa sarà da individuare in quella dello Stato in cui è ubicato lo stabilimento principale o lo stabilimento unico del Titolare del trattamento, anche per i trattamenti transfrontalieri eventualmente effettuati). Una volta determinata l'Autorità di Controllo competente, il Titolare del trattamento e il DPO individueranno la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Ente Parco Nazionale delle Foreste Casentinesi, Monte Falterona e Campigna dovrà provvedervi, senza ingiustificato ritardo. Quanto al contenuto di tale comunicazione, il Titolare del trattamento o da un suo delegato e il DPO dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o un suo delegato e il DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e-mail). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso ***DBR-ANALISI E VERBALE***, l'Ente Parco Nazionale delle Foreste Casentinesi, Monte Falterona e Campigna sarà tenuto a documentarlo.

Tale documentazione sarà affidata al Responsabile del Trattamento (o suo incaricato) con l'ausilio dell'Amministratore di Sistema Esterno dell'Ente (qualora la violazione riguardi dati contenuti in sistemi informatici), il quale dovrà provvedere altresì a tenere aggiornato il **MDP-RDB Registro dei Data Breach**, secondo le informazioni ivi riportate:

I. n. violazione;
II. data violazione;
III. natura della violazione;

IV. categoria di interessati;
V. categoria di dati personali coinvolti;
VI. numero approssimativo di registrazioni dei dati personali;
VII. conseguenze della violazione;
VIII. contromisure adottate;
IX. se sia stata effettuata notifica all'Autorità Garante Privacy (se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi ed il Titolare del Trattamento ne deve possedere una copia.

8. DOCUMENTAZIONE ALLEGATA

MDP-DBR DATA BREACH ANALISI E VERBALE

MDP-RDB REGISTRO DATA BREACH

ENTE PARCO NAZIONALE DELLE FORESTE CASENTINESI, MONTE FALTERONA E CAMPIGNA – DATA BREACH n.__ DEL _____

Breve descrizione della violazione del dato.

1. DATI GENERALI

Titolare del Trattamento: ENTE PARCO NAZIONALE DELLE FORESTE CASENTINESI, MONTE FALTERONA E CAMPIGNA

Responsabile della Protezione dei Dati Personali: Quality Management S.r.l.s

Gruppo di Lavoro:

2. NATURA DELLA VIOLAZIONE

Apertura Data Breach:

Avvenimento Data Breach:

Categorie degli Interessati:

Numero Interessati:

Categorie di Dati Personali Coinvolti:

Numero di Dati Personali Coinvolti:

3. DESCRIZIONE AVVENIMENTO ED AZIONI INTRAPRESE

Descrizione del Data Breach

SISTEMI COINVOLTI (sistemi di elaborazione e memorizzazione, compresa l'ubicazione):

AZIONI INTRAPRESE:

AZIONI DA INTRAPRENDERE:

4. RISCHIO DELLE LIBERTA' DEGLI INTERESSATI E REQUISITI DEI DATI VIOLATI

Considerato quanto sopra: Premessa

- RISERVATEZZA:
- INTEGRITA':
- DISPONIBILITA':

VALUTAZIONE: Esprimere la valutazione del rischio

5. POSSIBILI CONSEGUENZE

Descrivere le possibili conseguenze della violazione.

6. NOTIFICA AL GARANTE

Descrivere la motivazione della notifica al garante.

Se del caso, giustificare il motivo del ritardo (>72h)

7. NOTIFICA ALL'INTERESSATO

Descrivere la motivazione della notifica all'interessato e relativa modalità.

8. NOTE

Note.

CHIUSURA DATA BREACH:

FIRMA DEL RESPONSABILE DEL TRATTAMENTO

FIRMA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

MDP-RDB REGISTRO DATA BREACH									
N.	DATA RILEVA ZIONE	DESCRIZIONE (Riportare il n° del MDP-RDB)	ORIGINE	FUNZIONI COINVOLTE	TRATTA MENTO (Descrizi one)	AZIONE CORRETTIVA (Descrizione)	ESITO	DATA CHIUSURA	NOTE
