Direzione: DIREZIONE

Delibera del Presidente (con Firma Digitale)

N. **D00026** **del** **12/08/2020** **Proposta n.** 227 **del** 12/08/2020

Oggetto:

Modello organizzativo in materia di titolarità, responsabilità del trattamento e protezione dei dati personali della RNR Monte Navegna e Monte Cervia. Adozione.

Estensore

CARLONI VINCENZO

_____firma elettronica_____

Responsabile del Procedimento

LODOVISI VINCENZO

_____firma elettronica_____

Il Direttore

V. LODOVISI

_____firma digitale_____

Il Presidente

G. RICCI

_____firma digitale_____

Richiesta di pubblicazione sul BUR: NO

IL PRESIDENTE
Assunti i poteri del Consiglio

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;

VISTA la Legge Regionale 20 novembre 2001 n. 25, "Norme in materia di programmazione, bilancio e contabilità della regione", che definisce al Titolo VII, Capo I, artt. 56-60, la disciplina normativa da applicare agli Enti Pubblici dipendenti dalla Regione Lazio in materia di bilanci e rendiconti;

VISTO il Decreto del Presidente della Regione Lazio n° T00287 del 23/11/2018 di nomina del Presidente dell'Ente Regionale "Riserva Naturale Regionale Monte Navegna e Monte Cervia" nella persona del Sig. Giuseppe Ricci;

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 Decreto del Presidente della Regione Lazio n. T00094 dell' 8 giugno 2020, avente ad oggetto "Nomina Revisore dei conti unico e Revisore dei conti supplente della RNR Monte Navegna e Monte Cervia di cui all'art.15 della L.R. 6 ottobre 1997 n. 29, così come modificato dall'articolo 2, comma 15, lettera b), della legge regionale 14 luglio 2014, n. 7" con il quale è stato nominato Revisore dei conti unico dell'Ente il Dott. Luca Cervelli e Revisore dei conti supplente il dott. Mario Galasso;

VISTA la deliberazione del Presidente dell'Ente n. 21 del 24/09/2019, di adozione dello schema di Bilancio di previsione triennale 2020-2022 con i relativi allegati;

VISTA la L.R. 27/12/2019 n. 29 "Bilancio di previsione finanziario della Regione Lazio 2020-2022" con cui all'art. 6, ai sensi dell'art. 57 della L.R. 20 novembre 2001 n. 25 e ss. mm. e nel rispetto delle disposizioni riportate nell'art. 47, comma 5 del d.lgs. 118/2011, vengono approvati i bilanci di previsione per l'anno finanziario 2020 e pluriennale 2021-2022 deliberati dagli enti pubblici dipendenti dalla Regione fra cui quello della RNR Monte Navegna e Monte Cervia;

VISTA la legge regionale 18 febbraio 2002, n. 6, recante disposizioni concernenti la "Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale" e successive modificazioni;

VISTO il Regolamento regionale 6 settembre 2002, n. 1 "Regolamento di organizzazione degli uffici e dei servizi della giunta regionale" e successive modifiche;

VISTO il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di dati personali) e successive modifiche;

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 denominato Regolamento;

VISTA la legge 25 ottobre 2017, n. 163 (Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017) e, in particolare, l'articolo 13, ai sensi del quale il Governo è delegato all'adozione di uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento;

VISTA la "Rettifica 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)";

VISTO il Decreto Legislativo 10 agosto 2018, n. 101, intitolato "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 (regolamento generale sulla protezione dei dati)"; VISTA la "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali" del Garante per la protezione dei dati personali;

CONSIDERATO in particolare, il principio di "responsabilizzazione" ("accountability") che attribuisce, al titolare del trattamento, il compito di mettere in atto "misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento", alla luce "della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1. del RGPD);

RITENUTO, conseguentemente, di dover adottare un modello organizzativo all'interno dell'Ente che definiisca la ripartizione delle competenze, l'attuazione degli adempimenti previsti dalla normativa, i compiti assegnati al DPO, i criteri generali da rispettare nell'individuazione dei soggetti responsabili e autorizzati a compiere le operazioni di trattamento;

VISTO il documento "modello organizzativo in materia di protezione dei dati personali dell'Ente predisposto dagli Uffici e allegato alla presente deliberazione quale parte integrante e sostanziale;

VISTO l'art. 37 paragrafo 3 del sopracitato regolamento (UE) 2016/679 del Parlamento Europeo, che testualmente stabilisce: "Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione."

CONSIDERATO che, ai sensi dell'art. 37, par. 1 lettera a) del Regolamento (UE) 2016/679, occorre provvedere alla designazione del Responsabile della Protezione dei Dati, e che attualmente sono in corso di completamento, da parte della Direzione Regionale competente, le procedure di cui all'art. 37 paragrafo 3 del citato regolamento;

Tutto ciò premesso e considerato

DELIBERA

1. Di adottare il modello organizzativo in materia di titolarità, responsabilità del trattamento e protezione dei dati personali dell' Ente Riserva Naturale Regionale Monte Navegna e Monte Cervia, che allegato alla presente deliberazione ne costituisce parte integrante e sostanziale;

2. Di dare atto che con successivo atto si procederà alla designazione del D.P.O. Data Protection Officer per la protezione dei dati personali ai sensi dell'art. 37, par. 1 lettera a) del Regolamento europeo 679/2016 e s.m.i. per il periodo necessario al completamento, da parte della Direzione Regionale competente, delle procedure di cui all'art. 37 paragrafo 3 del regolamento (UE) 2016/679 del Parlamento Europeo citato in narrativa:

3. di trasmettere lo stesso al Direttore dell'Ente per gli atti conseguenti. 4. di disporre la pubblicazione del presente atto sul sito internet istituzionale nella sezione Amministrazione Trasparente, sotto sezione "Altri contenuti - Accessibilità e Catalogo di dati, metadati e banche dati" e sotto sezione "Provvedimenti".

Letto confermato e sottoscritto

ALLEGATO A)

MODELLO ORGANIZZATIVO IN MATERIA DI TITOLARITÀ, RESPONSABILITÀ DEL TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI DELL'ENTE RISERVA NATURALE REGIONALE MONTE NAVEGNA E MONTE CERVIA

1. Indirizzi generali

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 (di seguito "Regolamento") detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni. Le disposizioni del D.lgs. 196/2003 "Codice in materia di protezione dei dati personali", nonché i Provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante"), continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa succitata. Per dare attuazione ai suddetti obblighi ed adempimenti, l' Ente Riserva Naturale Regionale monte Navegna e Monte Cervia (di seguito Parco) rivede l'assetto delle responsabilità tenuto conto della propria organizzazione. Il Regolamento individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

- il titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

- il responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- il responsabile della protezione dei dati (di seguito "Data Protection Officer" o "DPO"): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;

- le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del art. 4 del Regolamento.

Con il presente documento il Parco definisce il proprio ambito di titolarità, la ripartizione delle competenze, l'attuazione degli adempimenti previsti dalla normativa; indica i compiti assegnati al DPO designato e definisce i criteri generali da rispettare nell'individuazione dei soggetti responsabili e autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità, come di seguito riportato.

2. Il Titolare del Trattamento

Titolare del trattamento di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è l'Ente Riserva Naturale Regionale monte Navegna e Monte Cervia, nella persona del legale rappresentante pro tempore, come individuato nella persona del Presidente, cui spetta, in particolare:

- adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi necessari;

- designare il Responsabile della Protezione Dati (DPO);

- designare i soggetti responsabili degli adempimenti previsti dalla normativa in materia di trattamento dati personali;

- istruire i soggetti autorizzati al trattamento dei dati personali;

- tenere un registro delle attività di trattamento svolte sotto la propria responsabilità;

- cooperare, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti;

- notificare, in caso di violazione dei dati personali, la violazione medesima all'autorità di controllo competente a norma dell'articolo 55 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;

- comunicare la violazione all'interessato, su segnalazione del responsabile, senza ingiustificato ritardo quando la medesima violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

- effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti, su segnalazione del responsabile, previsti sulla protezione dei dati personali quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

- consultare l'autorità di controllo, prima di procedere al trattamento, qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

- assicurarsi che i responsabili della protezione dei dati siano tempestivamente e adeguatamente coinvolti in tutte le questioni riguardanti la protezione dei dati personali;

- sostenere il DPO nell'esecuzione dei compiti fornendogli le risorse necessarie per assolverli;

- assicurarsi che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti;

- documentare ed è in grado di provare, in caso di richiesta dell'autorità di controllo, l'attuazione del sistema di sicurezza finalizzato alla protezione dei dati personali.

3. Responsabile del Trattamento

È designato quale Responsabile del trattamento dei dati personali effettuati dall'Ente, in esecuzione dell'art. 28 del Regolamento, il Direttore dell'Ente, cui sono affidati i seguenti compiti:

• collaborare con il personale per l'elaborazione degli obiettivi strategici e operativi nonché della pianificazione strategica del sistema di sicurezza e di protezione dei dati personali, sensibili e giudiziari;

• identificare eventuali contitolari, responsabili esterni e sub responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere gli accordi interni e i contratti per il trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi;

• identificare e designare, per iscritto e in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura organizzativa di competenza, le persone fisiche della struttura organizzativa medesima, c.d. Incaricati, che operano sotto la diretta autorità del titolare per il tramite del responsabile di competenza, e attribuire alle persone medesime specifici compiti e funzioni inerenti al trattamento dei dati, conferendo apposito incarico per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento, impartendo a tale fine specifiche istruzioni, e controllando costantemente che le persone fisiche designate e autorizzate effettuino le operazioni di trattamento:

- in attuazione del principio di «liceità, correttezza e trasparenza»;
- in attuazione del principio di «minimizzazione dei dati»;
- in attuazione del principio di «limitazione della finalità»;
- in attuazione del principio di «esattezza»; o in attuazione del principio di «limitazione della conservazione»;
- in attuazione del principio di «integrità e riservatezza»;
- in attuazione del principio di «liceità, correttezza e trasparenza»;

• provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;

• effettuare la ricognizione integrale di tutti i trattamenti di dati personali, sensibili e giudiziari svolti nella struttura organizzativa di competenza, in correlazione con i processi/procedimenti svolti dall'Ufficio;

• effettuare l'aggiornamento periodico, e comunque in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;

• effettuare l'analisi del rischio dei trattamenti, e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli interessati;

• effettuare, prima di procedere al trattamento, quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una valutazione dell'impatto del trattamento sulla protezione dei dati personali;

• mettere in atto le misure tecniche e organizzative adeguate e funzionali a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

• mettere in atto le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, fermo restando che:

- tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità;
- dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica;

• proporre e suggerire al titolare misure tecniche e organizzative ritenute necessarie garantire la protezione dei dati dal trattamento, in relazione ai trattamenti della struttura organizzativa di competenza;

• gestire il registro delle attività di trattamento in relazione ai trattamenti della struttura organizzativa di competenza;

• cooperare, su richiesta, con il DPO e con l'Autorità di controllo nell'esecuzione dei suoi compiti;

• garantire al responsabile del Servizio ICT e al DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza;

• in caso di violazione dei dati personali, collaborare con il titolare e il DPO per notificare la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro72 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;

• prima di procedere al trattamento, consultare l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

• assicurarsi che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;

• sostenere il DPO nell'esecuzione dei compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;

• documentare ed essere in grado di provare, in caso di richiesta dell'Autorità di controllo, l'attuazione del sistema di sicurezza finalizzato alla protezione dei dati personali;

• collaborare con il titolare per l'inserimento dei rischi di corruzione, illegalità e degli illeciti in materia di trattamento di dati personali negli aggiornamenti annuali al PTPC e collaborare al RPCT per le segnalazioni degli illeciti relativi al trattamento dei dati;

• collaborare con i dirigenti per l'elaborazione e l'aggiornamento delle procedure necessarie al sistema di sicurezza e, in particolare per la procedura da utilizzare in caso di data breach;

• controllare e monitorare la conformità dell'analisi, della valutazione dei rischi, e della valutazione di impatto nonché controllare e monitorare la conformità del trattamento dei rischi al contesto normativo, regolamentare, gestionale, operativo e procedurale, con obbligo di tempestiva revisione in caso di rilevazioni di non conformità o di scostamenti;

• conformare il trattamento ai pareri e indicazioni del DPO e dell'Autorità di controllo nonché alle linee guida e ai provvedimenti dell'Autorità di controllo;

• formulare proposte, in occasione dell'approvazione/aggiornamento degli strumenti di pianificazione e programmazione, volte ad implementare il sistema di sicurezza e ad elevare il livello di protezione degli interessati;

• richiamare obbligatoriamente nei contratti di sviluppo software e piattaforme, la policy in materia di sviluppo delle applicazioni, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per la Provincia di risoluzione del contratto;

• promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione come valore da integrare in ogni processo/procedimento;

• effettuare ogni ulteriore attività, non espressamente indicata in precedenza e necessaria per la integrale attuazione del Regolamento e della normativa interna di adeguamento.

4. I Responsabili Esterni

Sono, inoltre, designati responsabili del trattamento di dati personali i soggetti esterni al Parco di che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del Titolare. Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata anche valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché il medesimo sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

5. Gli Incaricati

Sono autorizzati al compimento alle operazioni di trattamento dei dati, oltre ai Responsabili del trattamento, i dipendenti e collaboratori a qualsiasi titolo dai medesimi individuati e che operano sotto la loro diretta responsabilità, che conformano i loro trattamenti alla policy dell'Ente in materia di protezione dei dati personali e alle istruzioni di seguito riportate, che costituiscono cogenti prescrizioni, anche ai fini della responsabilità personale:

• in attuazione del principio di «liceità, correttezza e trasparenza», raccolta, registrazione, elaborazione di dati, agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati presenti nell'Ufficio di appartenenza, nell'osservanza delle tecniche e metodologie in atto;

• in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui la persona fisica designata al trattamento è preposta;

• in attuazione del principio di «limitazione della finalità», trattamento conforme alle finalità istituzionali del titolare e limitato esclusivamente a dette finalità;

• in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, e obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;

• in attuazione del principio di «limitazione della conservazione», obbligo di conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello

necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati e obbligo di esercitare la dovuta diligenza affinché non vengano conservati nell'Ufficio di competenza dati personali non necessari o divenuti ormai superflui. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti dati sensibili vengano conservati in contenitori/armadi muniti di serratura o in ambienti ad accesso selezionato e vigilato, fino alla restituzione;

• in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente e integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati illeciti e dalla perdita, dalla distruzione o dal danno accidentali;

• in attuazione del principio di «liceità, correttezza e trasparenza», autorizzazione a comunicare eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal titolare del trattamento.

• Le medesime istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici e informatici, contenuti in archivi/banche dati o destinati a figurarvi. In particolare, per tali trattamenti, la persona fisica designata e incaricata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

o Password e username Conservare e custodire personalmente le credenziali di autenticazione informatiche di accesso affidate dal Parco in relazione al trattamento dati assegnato, che non possono essere condivise con altri incaricati del trattamento.

o Logout La persona fisica designata al trattamento, al termine di ogni sessione di trattamento ha l'obbligo di terminare la sessione scollegandosi opportunamente dall'applicazione utilizzata effettuando il logout.

- Supporti di tipo magnetico e/o ottico

La persona fisica designata al trattamento, ha l'obbligo di:

• verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;

• evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;

• rivolgersi tempestivamente, per difficoltà o questione inerente la sicurezza, al proprio dirigente responsabile.

6. Il Responsabile della Protezione dei Dati (DPO)

Il Regolamento prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (DPO). Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli artt. 37 e ss. del Regolamento, conformati alla precipua organizzazione dell'Ente:

• informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali;

• sorveglia l'osservanza della normativa nonché delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

• coopera con il Garante per la protezione dei dati personali;

• funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;

• partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del Servizio ICT competente o ne richiede di specifiche;

• promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;

• partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente;

• formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento.

• fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.

7. Pareri del DPO

Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'Ente presentano nei casi di seguito indicati. Pareri obbligatori Devono essere obbligatoriamente richiesti pareri in ordine a:

• individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, anche a seguito di incidenti di sicurezza o analisi dei rischi;

• adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;

• individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali; incidenti sicurezza. Pareri facoltativi Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

• progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;

• valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento;

• valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento;

• opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

• Le richieste di parere devono essere inviate all'indirizzo di posta elettronica direzione@navegnacervia.it nelle modalità stabilite del Parco. I pareri sono espressi nel rispetto delle seguenti codifiche:

• NC: acronimo di “non conformità”, nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;

• OS: acronimo di “osservazione”, nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;

• PO: acronimo di “positivo”, nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy regionali in materia di protezione dei dati personali. Nei casi in cui il DPO esprima pareri “NC” e “OS” il titolare deve formalizzare, nelle medesime forme utilizzate dal DPO per l’espressione del parere, le motivazioni che giustificano l’esecuzione dell’attività o l’implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal DPO. I pareri espressi dal DPO sono conservati agli atti.

8. Il Servizio ICT competente

Il Servizio competente in materia di sistemi informativi e di sicurezza informatica svolge un ruolo di supporto al DPO in tema di risorse strumentali e di competenze. Al fine di adeguare le funzioni assegnate con la designazione della nuova figura del DPO è necessario prevedere per il Servizio i compiti di seguito meglio specificati:

• individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell’Ente. Tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del DPO;

• condivide le evidenze dell’analisi dei rischi con il DPO, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;

• provvede, ogni qualvolta venga avvertito un problema di sicurezza a:

- attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;
- individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO;
- segnalare al responsabile competente in materia di sistemi informativi le violazioni dei dati personali ai fini della notifica, ai sensi dell’art. 33 del Regolamento, al Garante per la protezione dei dati personali;
- svolgere verifiche sulla puntuale osservanza della normativa e delle policy in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste del medesimo;
- promuovere la formazione di tutto il personale dell’Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all’interno della Ente, coordinandosi con le azioni promosse dal DPO.

Al Servizio competente in materia di sistemi informativi e di sicurezza informatica spetta, inoltre:

• l’adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all’utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare ogni qualvolta l’evoluzione tecnica o normativa lo renda necessario;

• la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

9. Accesso civico generalizzato e ruolo DPO

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il DPO, le strutture dell'Ente, e il Responsabile per la Prevenzione della Corruzione e Trasparenza (R.P.C.T.). Il D.Lgs. 97/2016, di modifica del D.lgs. 33/2013 ha introdotto l'istituto dell'accesso civico "generalizzato", che attribuisce a chiunque il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione. L'esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del d.lgs. n. 33/2013. L'art. 5, comma 5, d.lgs. n. 33/2013 prevede infatti che, per ciascuna domanda di accesso generalizzato, l'amministrazione debba verificare l'eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria. Il DPO funge da supporto alle strutture competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e, comunque, per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato. Il DPO funge altresì da supporto al R.P.C.T. nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali. Il DPO, inoltre, su richiesta delle strutture, esprime proprio parere in ordine alla valutazione dell'eventuale pregiudizio che l'accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016. Il DPO, su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti. Sulla scorta di tale parere le strutture competenti sulle singole richieste di accesso effettueranno il bilanciamento tra gli interessi asseritamente lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.