Disciplinare di gestione della Sicurezza delle informazioni esplicativo del GDPR

Il presente Disciplinare è stato emesso con numero di revisione 01 per l'Ente Regionale RomaNatura

STORIA DEL DOCUMENTO

Rev.	Motivo del cambiamento
01	PrimaStesura

Indice

L'Ente Regionale RomaNatura ha redatto il presente documento al fine di poter stabilire obblighi e responsabilità in merito alla gestione della privacy secondo la normativa cogente.

1 Scopo del GDPR (General Data ProtectionRegulation)

Scopo di questo Documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi in materia di sicurezza del trattamento dei dati effettuato dall'Ente Regionale "RomaNatura" con sede in Via Gomenizza n. 81 — 00195 Roma, Codice Fiscale 97153420589, Partita IVA 07071371004 (nel seguito del Documento indicato come Titolare) previsti dal D.lgs. 196/2003 "Codice in materia di protezione dei dati personali» nonché definite dal Regolamento 679/2016 e adottate dalla Società Roma Natura per assicurare che il trattamento dei dati personali acquisiti nell'ambito delle attività di lavoro della Società siano gestiti nel rispetto degli obblighi previsti dalla regolamentazione europea e dalle leggi nazionali vigenti e, le deliberazioni della COMMISSIONE e del GARANTE per la Privacy.

Il tutto finalizzato a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

Il Documento Programmatico sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali (comuni, sensibili e giudiziari) effettuato per mezzo di strumenti elettronici di elaborazione e di strumenti non elettronici di elaborazione (cartacei, audio, visivi, audiovisivi, etc.). Deve essere conosciuto ed applicato da tutti i Settori che fanno parte dell'Ente.

2 Soggetti di riferimento per il GDPR

L'Ente Regionale RomaNatura, in accordo con l'articolo 1 del Reg. 679/2016, ritiene che oggetto delle disposizioni del presente disciplinareGDPR sia tutta la serie di attività predisposte alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alle norme relative alla libera circolazione dei dati personali.

Esso tutela i diritti e le libertà fondamentali delle persone fisiche e in particolare il loro diritto alla protezione dei dati personali. Sottolinea inoltre che la libera circolazione dei dati personali all'interno dell'UnioneEuropea non deve essere né limitata né vietata per motivi connessi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali che devono comunque essere protetti e tutelati secondo la lettera della legge.

3 Quadro Normativo Di Riferimento

- D.lgs. n. 196/2003 (Codice in materia di dati personali)
- Allegato B al D.lgs. 196/2003 (Disciplinare Tecnico in materia di Misure Minime di
- Sicurezza)
- Regolamento Europeo 679/2016 sulla General Data Protection Regulation
- Convenzione 108 del CE

4 Struttura Del Documento

Conformemente a quanto prescrive il Regolamento Europeo 679/2016, l'Ente Regionale Roma Natura nel presente disciplinare delinea idonee informazioni riguardanti:

1. vari trattamenti di dati personali mediante:

a. elencazione dei soggetti che trattano i dati, la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;

b. individuazione dei tipi di dati personali trattati;

2. distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte dai regolamenti sul trattamento dei dati;

3. analisi dei rischi che incombono sui dati

4. misure già adottate e da adottare per garantire l'integrità e la disponibilità dei dati;

5. criteri e le modalità di recupero dei dati, in seguito a danneggiamento e distruzione;

6. previsione di interventi formativi degli incaricati del trattamento;

7. criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rilevare lo stato di salute e la vita sessuale.

5 Definizioni

Al fine di poter comprendere al meglio i termini utilizzati all'interno del presente disciplinare l'Ente Regionale RomaNatura elenca di seguito i termini ed il significato loro attribuito, all'interno del documento stesso:

- "Dati personali": qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"); una persona fisica identificabile è colui che può essere identificato, direttamente o indirettamente, in particolare facendo riferimento a un identificatore come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o uno o più fattori specifici per l'aspetto fisico, fisiologico, identità genetica, mentale, economica, culturale o sociale di quella persona naturale;
- "Dato Anonimo": dato che, in origine o a seguito di trattamento, non può essere associato ad un Interessato.
- "Dato identificativo": dato personale che permette l'identificazione diretta dell'interessato
- "Dato sensibile": dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché dato personale idoneo a rivelare lo stato di salute e la vita sessuale.
- "Dato giudiziario": dato personale idoneo a rivelare provvedimenti in materia di
  - casellario giudiziale,
  - di anagrafe delle sanzioni amministrative dipendenti da reato e
  - di relativi carichi pendenti,
  - della qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di Procedura Penale
- "Trattamento": qualsiasi operazione o insieme di operazioni eseguite su dati personali o su serie di dati personali, anche con strumenti automatizzati, quali raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, recupero, consultazione, uso, divulgazione per trasmissione, diffusione o altrimenti messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione;
- "Limitazione del trattamento":la marcatura di dati personali memorizzati al fine di limitare il loro trattamento in futuro;
- "Profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'uso di dati personali per valutare determinati aspetti personali relativi a una persona fisica, in

particolare per analizzare o prevedere aspetti riguardanti le prestazioni di tale persona fisica sul luogo di lavoro,appartenenza politica o sindacale, la situazione economica, la salute, preferenze personali, interessi, affidabilità, comportamento, posizione o movimenti;

- "Pseudonimizzazione": il trattamento di dati personali in modo tale che i dati personali non possono più essere attribuiti a un interessato specifico senza l'uso di ulteriori informazioni, a condizione che tali informazioni aggiuntive siano conservate separatamente e siano soggette a misure tecniche e organizzative atte a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- "Banca Dati":qualsiasi insieme strutturato di dati personali accessibili in base a criteri specifici, centralizzati, decentrati o dispersi su base funzionale o geografica;
- "Controllore": la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che, da solo o congiuntamente con altri, determina le finalità e i mezzi del trattamento di dati personali; se le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o dello Stato membro, il responsabile del trattamento o i criteri specifici per la sua nomina possono essere previsti dalla legislazione dell'Unione o dello Stato membro;
- "Titolare del Trattamento": la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati,ivi compreso il profilo della sicurezza.
- "Responsabile del trattamento": la persona fisica, la persona giuridica, la pubblica amministrazione equalsiasi altro ente, associazione od organismo nominati dal titolare al trattamento di dati personali. Ladesignazione di un responsabile non esonera da responsabilità il titolare, il quale deve impartirgli compiti e precise istruzioni e deve vigilare sull'attuazione di questi. Ilresponsabile deve essere un soggetto che conferisce idoneagaranzia del pieno rispetto delle disposizioni delle normative di regolamentazione sulla Pirvacy, ivi compreso il profilorelativo alla sicurezza.
- "Incaricato del trattamento": persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che tratta dati personali per conto del responsabile del trattamento;
- "Interessato": la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
- "Destinatario": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo a cui vengono comunicati i dati personali, sia che si tratti di terzi o meno. Tuttavia, le autorità pubbliche che possono ricevere dati personali nel quadro di un'indagine particolare in conformità del diritto dell'Unione o dello Stato membro non sono considerati destinatari; il trattamento di tali dati da parte di tali autorità pubbliche deve essere conforme alle norme applicabili in materia di protezione dei dati conformemente alle finalità del trattamento;
- "Terza parte": una persona fisica o giuridica, autorità pubblica, agenzia o organismo diverso dall'interessato, responsabile del trattamento, incaricato del trattamento e persone che, sotto l'autorità diretta del responsabile del trattamento o dell'incaricato del trattamento, sono autorizzate a trattare dati personali;
- "Consenso" dell'interessato: qualsiasi indicazione liberamente concessa, specifica, informata e inequivocabile dei desideri della persona interessata con la quale egli o lei, mediante una dichiarazione o una chiara azione affermativa, implica l'accordo sul trattamento dei dati personali relativi a lui o lei;
- "Violazione dei dati personali": violazione della sicurezza che comporta distruzione, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato a dati personali trasmessi, archiviati o altrimenti trattati;
- "Dati genetici": dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni uniche sulla fisiologia o sulla salute di tale persona fisica e che derivano, in particolare, dall'analisi di un campione biologico dal persona fisica in questione;
- "Dati biometrici": dati personali risultanti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che consentono o

confermano l'identificazione univoca di tale persona fisica, quali immagini facciali o dati dattiloscopici;

- "Dati relativi alla salute": dati personali relativi alla salute fisica o mentale di una persona fisica, compresa la fornitura di servizi di assistenza sanitaria, che rivelano informazioni sul suo stato di salute;
- "Stabilimento principale":è il luogo dove risiede l' amministrazione centrale (del titolare e/o del responsabile del trattamento) nell'Unione salvo che le decisioni sulle finalità e i mezzi del trattamento di dati siano adottate in un altro stabilimento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni;
- "Rappresentante": una persona fisica o giuridica stabilita nell'Unione che, designata dal responsabile del trattamento o incaricato del trattamento per iscritto a norma dell'articolo 27, rappresenta il responsabile del trattamento o l'incaricato del trattamento in relazione ai rispettivi obblighi ai sensi del regolamento 679/2016;
- "Norme aziendali vincolanti": le politiche di protezione dei dati personali che sono rispettate da un responsabile del trattamento o incaricato del trattamento stabilito nel territorio di uno Stato membro per trasferimenti o una serie di trasferimenti di dati personali a un responsabile del trattamento o incaricato del trattamento in uno o più paesi terzi gruppo di imprese o gruppo di imprese impegnate in un'attività economica comune;
- "Autorità di controllo": un'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- "Autorità di controllo interessata": un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    - il responsabile del trattamento o l'incaricato del trattamento è stabilito nel territorio dello Stato membro di tale autorità di controllo;
    - le persone interessate che risiedono nello Stato membro di tale autorità di controllo sono sostanzialmente interessate o possono essere sostanzialmente interessate dal trattamento;
    - una denuncia è stata presentata a tale autorità di controllo;
- "Obiezione pertinente e motivata", un'obiezione a un progetto di decisione relativa alla presenza di una violazione del regolamento 679/2016, a condizione che l'azione prevista nei confronti del responsabile del trattamento o dell'incaricato del trattamento sia conforme al regolamento stesso, le documentazioni siano in grado di dimostrare chiaramente l'importanza dei rischi presentati, il processo di decisione riguardante i diritti e le libertà fondamentali delle persone interessate e, se del caso, il libero flusso di dati personali all'interno dell'Unione;
- "Servizio della società dell'informazione": un servizio quale definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- "Organizzazione internazionale": un'organizzazione e i suoi organismi subordinati di diritto pubblico internazionale o qualsiasi altro organismo costituito da, o sulla base di un accordo tra due o più paesi.
- "Comunicazione":dare conoscenza dei dati personali in qualunque forma, anche mediante la loro messa a disposizione o consultazione, a uno o più soggetti che sono diversi dalle figure predisposte nel presente disciplinare, e quindi diverse dall'interessato, dal titolare, dal responsabile e dagli incaricati.
- "Diffusione": dare conoscenza dei dati personali a soggetti indeterminati, ovvero soggetti non identificabili, in qualunque forma, anchemediante la loro messa a disposizione o consultazione
- "Blocco": la conservazione di dati con sospensione temporanea di ogni altra operazione del trattamento.

6 Ambito di applicazione ed esenzione

L'Ente Regionale RomaNatura applica il presente disciplinare a tutti gli elaborati elettronici e supporti cartacei che fanno parte di un sistema di archiviazione o che sono destinati a far parte di un sistema di

archiviazione,a tutti gli Incaricati, gli eventuali Responsabili, i Titolari del trattamento ed a tutto il personale coinvolto, a vario titolo, nelle sessioni di trattamento dati effettuati per nome e per conto dell'Ente.

In accordo con l'articolo 2 del Reg.679/2016, l'Ente Regionale RomaNatura non applica il presente disciplinare al trattamento di dati personali:

- nel corso di un'attività che esula dall'ambito di applicazione del diritto dell'Unione;
- degli Stati membri nello svolgimento di attività che rientrano nell'ambito di applicazione del capo V del titolo V del TUE;
- di una persona fisica nel corso di un'attività puramente personale o domestica;
- delle autorità competenti ai fini della prevenzione, dell'indagine, dell'individuazione o del perseguimento di reati o dell'esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.
- per il trattamento di dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali sono adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.

Il presente disciplinare,non pregiudica l'applicazione della direttiva 2000/31/CE, in particolare delle norme sulla responsabilità dei fornitori di servizi di intermediazione di cui agli articoli da 12 a 15 di tale direttiva.

7 Ambito di applicazione territoriale

L'Ente Regionale RomaNatura in accordo con l'Art 3 del Reg.679/2016 applica le disposizioni del presente disciplinare al trattamento dei dati personali nell'ambito delle attività di tutte le sedi e di tutti i locali in uso dall'Ente (titolare del trattamento),indipendentemente dal fatto che il trattamento avvenga nell'Unione o meno.

Il presente disciplinare è applicabile sia al trattamento dei dati personali degli interessati che si trovano nell'Unione, da parte di un responsabile del trattamento o di un incaricato del trattamento anche se non è stabilito nell'Unione, per cui le attività di trattamento sono connesse a:

- l'offerta di beni o servizi, a prescindere dal fatto che sia richiesto un pagamento all'interessato;
- il monitoraggio del loro comportamento all'interno dell'Unione;
- il trattamento di dati personali da parte di un responsabile del trattamento non stabilito nell'Unione, ma in un luogo in cui il diritto degli Stati membri si applica in virtù del diritto pubblico internazionale.

8 Principi generali del GDPR

Il GDPR dell'Ente Regionale RomaNatura si basa su alcuni principi generali sia del nuovo Regolamento 679/2016 sia su alcune parti del D.Lgs 196/2003 che ad oggi non risultano né sostituite né abrogate dal nuovo regolamento.
Questi principi, relativi alla modalità del trattamento ed ai requisiti dei dati, affermano che i dati devono essere:

1. trattati in modo lecito, equo e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
2. raccolti per scopi determinati, espliciti e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi; l'ulteriore trattamento ai fini dell'archiviazione nell'interesse pubblico, a fini di ricerca scientifica o storica oa fini statistici, conformemente all'articolo 89, paragrafo 1, non è considerato incompatibile con le finalità iniziali ("limitazione delle finalità");
3. adeguati, pertinenti e limitati a quanto necessario in relazione agli scopi per i quali sono trattati ("minimizzazione dei dati");

4. accurati e, se necessario, aggiornati; deve essere infatti adottato ogni ragionevole sforzo per garantire che i dati personali che sono inaccurati o inesatti, tenendo conto delle finalità per cui sono trattati, siano cancellati o rettificati senza indugio ("accuratezza");
5. tenuti in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario agli scopi per i quali i dati personali sono trattati; i dati personali possono essere conservati per periodi più lunghi nella misura in cui i dati personali saranno trattati unicamente a fini di archiviazione nell'interesse pubblico, a fini di ricerca scientifica o storica oa fini statistici ai sensi dell'articolo 89, paragrafo 1,fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
6. elaborati in modo tale da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro l'elaborazione non autorizzata o illecita e contro la perdita accidentale, la distruzione o il danneggiamento, ricorrendo a misure tecniche o organizzative appropriate ("integrità e riservatezza").

L'Ente Regionale RomaNatura ha incaricato il responsabile del trattamento in accordo ai requisiti di conformità al paragrafo 1 ("responsabilità") del Regolamento 679/2016.

Al fine di ottemperare al meglio alle indicazioni cogenti il presente disciplinare prevede inoltre:

- l'obbligo di un registro di tenuta dei trattamenti definito GDPR (General Data Protection Regulation – Regolamento UE 2016/679)
- l'obbligo generalizzato di notifica al Garante per le violazioni della sicurezza dei dati;
- l'obbligo di valutazione d'impatto sulla protezione dei dati con conseguente consultazione preventiva del Garante in caso di rischio elevato per i diritti e le libertà;
- l'obbligo della designazione di un DPO - Data Protection Officer -

9 Principi di base per la gestione del Trattamento in favore dell'Interessato (requisiti di necessità)

Il trattamentodel dato è lecito solo se e nella misura in cui si applica almeno una delle seguenti condizioni:

1. l'interessato ha prestato il consenso al trattamento dei propri dati personali per uno o più scopi specifici;
2. il trattamento è necessario per l'esecuzione di un contratto a cui l'interessato è parte o per prendere provvedimenti su richiesta dell'interessato prima di stipulare un contratto;
3. il trattamento è necessario per il rispetto di un obbligo legale a cui è soggetto il responsabile del trattamento;
4. il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica;
5. il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri conferiti al responsabile del trattamento, o istituzionalmente all'Ente;
6. il trattamento è necessario ai fini degli interessi legittimi perseguiti dal responsabile del trattamento o da un terzo, salvo il caso in cui tali interessi siano superati dagli interessi o dai diritti e dalle libertà fondamentali dell'interessato, che richiedono la protezione dei dati personali, in particolare quando il soggetto è un bambino.

Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente disciplinare per quanto riguarda il trattamento del dato. In questo modo si determinano con maggiore precisione requisiti specifici per il trattamento e/o altre misure per assicurare un trattamento lecito ed equo anche per altre situazioni di trattamento specifiche.
L'ordine di priorità delle leggi pone al primo posto il Diritto dell'Unione; successivamente la legge dello Stato membro a cui è soggetto il responsabile del trattamento.

10 Necessità del Trattamento

Lo scopo del trattamento è determinato dalla necessità che esso debba essere necessario ed indispensabile per l'esecuzione di un compito di interesse pubblico o nell'esercizio di autorità conferita al controllore.
Tale base giuridica può contenere disposizioni specifiche per adeguare l'applicazione delle norme del regolamento 679/2016, tra cui:

1. le condizioni generali che disciplinano la liceità del trattamento da parte del responsabile del trattamento;
2. i tipi di dati che sono soggetti al trattamento;
3. gli interessati;
4. le entità e i fini per i quali i dati personali possono essere divulgati;
5. la limitazione delle finalità;
6. i periodi di conservazione;
7. le operazioni di trattamento e le procedure di trattamento, comprese le misure volte a garantire un trattamento lecito ed equo.

L'Unione o la legge dello Stato membro devono quindi soddisfare un obiettivo di interesse pubblico e l'acquisizione del dato, deve essere proporzionale allo scopo legittimo perseguito.

Se il trattamento per uno scopo diverso da quello per il quale sono stati raccolti i dati personali non è basato sul consenso dell'interessato o su una legge dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democratica, il controllore tiene conto, tra l'altro, per stabilire se la trasformazione per un altro scopo sia compatibile con lo scopo per il quale i dati personali sono inizialmente rilevati,:

- di qualsiasi collegamento tra le finalità per le quali sono stati raccolti i dati personali e gli scopi dell'ulteriore trattamento previsto;
- del contesto in cui sono stati raccolti i dati personali, in particolare per quanto riguarda la relazione tra gli interessati e il responsabile del trattamento;
- della natura dei dati personali, in particolare se sono trattate categorie speciali di dati personali, ai sensi dell'articolo 9, o se sono trattati dati personali relativi a condanne penali e reati, ai sensi dell'articolo 10;
- delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- dell'esistenza di garanzie appropriate, che possono includere la crittografia o la pseudonimizzazione.

11 Revisione e validità del presente disciplinare

Il presente disciplinare è valido fino a quando gli elementi dell'Ente che intervengono durante il corso del trattamento dei dati non subiscono variazioni. Nel momento in cui uno o più elementi subissero variazioni, il presente disciplinare dovrà essere immediatamente revisionato con i dovuti aggiornamenti sulle variazioni e portato a conoscenza ~~del~~ di tutto il personale.

In ogni caso, il presente disciplinare dovrà essere aggiornato ed implementato immancabilmente con cadenza annuale.

Gli aggiornamenti devono tenere primariamente presente anche i livelli di rischio a cui sono soggetti i dati personali, comuni, sensibili e giudiziari nonché eventuali modifiche della tecnologia informatica.

12 Struttura Organizzativa dell'Azienda e sua Storia

L'Ente Regionale RomaNatura è l'Ente Regionale per la Gestione del Sistema delle Aree Naturali Protette nel Comune di Roma. Nato in attuazione della Legge Regionale n.29 del 6 ottobre 1997, RomaNatura è un Ente di diritto pubblico dotato di autonomia amministrativa, finanziaria e patrimoniale

. ….Omissis …..

I dati identificativi di Roma Natura possono essere così sintetizzati:

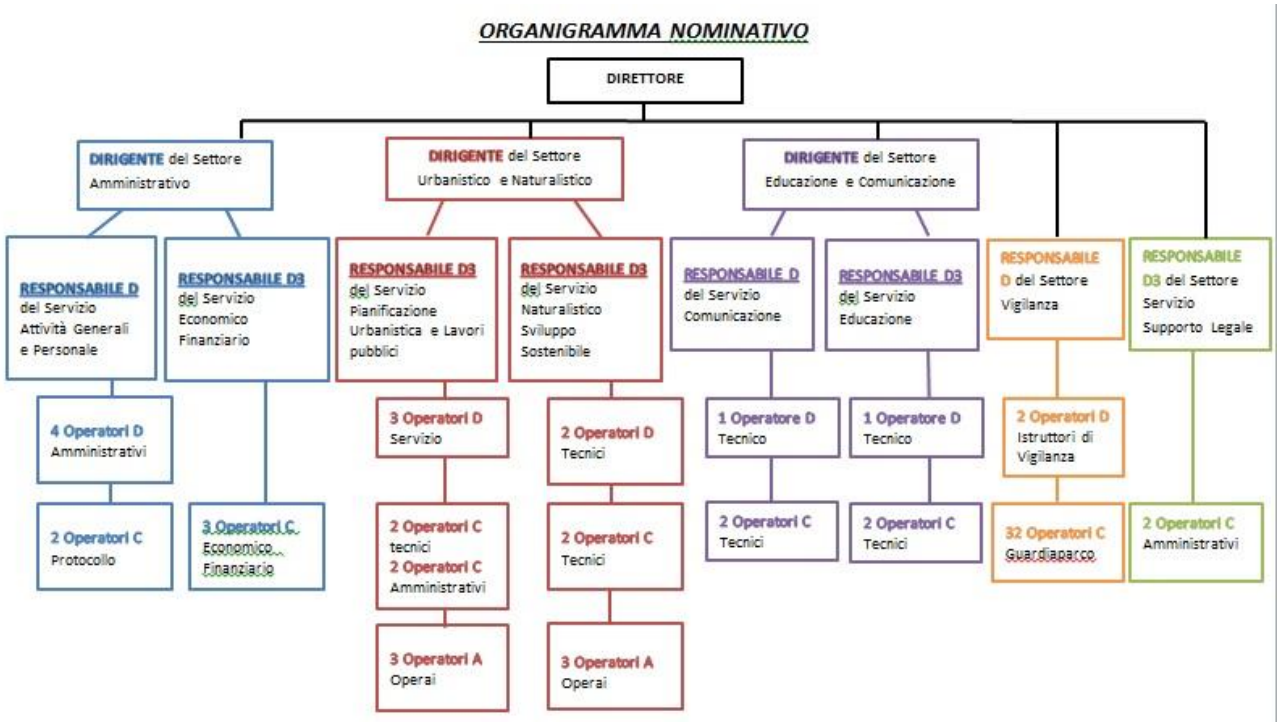
- SEDE LEGALE, AMMINISTRATIVA E COMMERCIALE — "Villa Mazzanti" Riserva Naturale di Monte Mario via Gomenizza, 81 – 00195 Roma
- SEDE OPERATIVA — "Villa Mazzanti" Riserva Naturale di Monte Mario via Gomenizza, 81 – 00195 Roma
- CODICE FISCALE — 97153420589
- PARTITA IVA — 07071371004
- TELEFONO — 06.35405345
- FAX — 06.35458539
- E-MAIL — privacy@romanatura.roma.it
- PEC — protocollo@pec.romanatura.roma.it

Sedi Operative secondarie:

Denominazione Sede	Indirizzo
Casa del Parco R.N.	Marcigliana Via di Tor San Giovanni n. 301 (Casale Lucerna i)
Casa del Parco R.N. Decima Malafede	Via Valle di Pema n. 315 (Torre di Perna)
Casa del Parco Valle dei Casali	Via del Casaletto n. 400
Casale Mellini	Viale del Parco Mellinisnc (Casale Mellini)
Casa del Mare	Via del Canale di Castelfusano n. I1

Struttura Interna- organigramma Privacy

L'organigramma del sistema dell'Ente Regionale RomaNatura è riportato come allegato al presente disciplinare:



L'intero sistema di gestione dell'Ente Regionale RomaNatura si basa sulle indicazioni contenute nello Statuto dell'Ente stesso, istituito dall'art.40 della Legge Regionale n. 29/97. L'Ente Regionale RomaNatura è Ente Regionale di diritto pubblico non economico, sottoposto alla vigilanza della Giunta Regionale ai sensi dell'articolo 55 dello Statuto Regionale.Le finalità perseguite dall'Ente Regionale RomaNatura, sono definite dall'articolo 3 della legge regionale n. 29/97 e possono essere riassunte nei seguenti punti:

1. Promuovere la tutela, il recupero, il restauro, la valorizzazione, le singolarità geologiche degli habitat naturali che abbiano rilevante valore naturalistico ed ambientale;
2. Promuovere, orientare ed esercitare attività scientifiche, didattiche e turistiche volte a favorire la conoscenza del Patrimonio ambientale dell'Area protetta e la sua corretta fruizione;
3. Individuare i criteri di compatibilità per la valutazione di opere ed interventi urbanistici che interferiscono con l'area protetta;
4. Rilascio di nulla osta, pareri, altri eventuali atti di assenso ad attività di trasformazione ambientale, territoriale ed urbanistica;
5. Concorrere a promuovere tutte le iniziative dirette a prevenire ed eliminare l'abusivismo edilizio e di degrado ambientale per inquinamento;
6. Accettare elargizioni e liberalità di qualsiasi forma vantaggiose per l'Ente Regionale RomaNatura;
7. Gestire il patrimonio dell'Ente sia in proprietà che in affidamento, esercitando nei modi previsti il diritto di prelazione su beni rilevanti a fini istituzionali;
8. Gestire i servizi dell'area naturale protetta con esclusione della vigilanza, anche tramite la stipula di convenzioni;
9. Aderire ad associazioni locali, regionali e nazionali per la promozione dei propri interessi istituzionali;
10. Stimolare l'interesse privato al finanziamento di opere ed interventi compatibili;

11. Promuovere qualsiasi atto utile al raggiungimento dei fini istituzionali.
12. Esercitare le proprie funzioni in accordo con gli Enti Parco e con il coordinamento della Direzione Regionale Capitale Naturale Parchi ed Aree Protette in ottica di Sistema.

Inoltre l'Ente Regionale RomaNatura promuove forme di consultazione delle popolazioni locali al fine di garantire la partecipazione dei cittadini alle attività dell'Ente. Il cittadino può rivolgere petizioni per chiedere provvedimenti o esporre necessità.

L'Ente garantisce il diritto di accesso all'informazione ambientale e la sistematica e progressiva messa a disposizione del pubblico.

La gestione delle sopra elencate attività istituzionali, comporta spesso l'acquisizione di dati identificativi, sensibili e giudiziari. Tali dati sono gestiti, organizzati e conservati secondo quanto indicato dalla vigente normativa sulla tutela della privacy.

In particolare con riferimento agli atti dispositivi che comportano l'acquisizione istituzionale di dati identificativi, le attività di riferimento, possono essere così elencate:

Settore amministrativo:
- Redazione di mandati di pagamento e delle reversali di incasso
- Redazione di Bandi e gare d'appalto relative a fornitura di servizi e acquisto di beni per le attività generali e di funzionamento dell'Ente e adempimenti correlati

Settore tecnico urbanistico e naturalistico:
- Rilascia Pareri/Nulla Osta in merito al recupero del patrimonio edilizio rurale (PUA, PUMA)
- Ordinanze di sospensione lavori
- Ordinanze di ripristino dello stato dei luoghi ai sensi dell'art.28 co.3 della L.R. n. 29/97
- Atti relativi ai procedimenti espropriativi di competenza, ai sensi dell'art6, commi 1 e 9 del DPR 327/2001
- Redazione di Bandi e gare d'appalto relative a lavori pubblici e manutenzioni e adempimenti correlati
- Stesura di perizia estimativa di pratiche indennizzo dei danni da fauna selvatica
- Rilascio Nulla Osta ambientali: vegetazione, difesa del suolo, acque
- Rilascio Nulla Osta tagli boschivi
- Rilascio Nulla Osta verde urbano
- Rilascio Parere per nulla Osta di aziende agricole
- Rilascio Parere in merito a problematiche di tutela archeologica

Settore tecnico educazione e comunicazione:
- Redazione degli atti per la stipula di contratti e/o Convenzioni
- Redazione di Bandi e gare d'appalto relative a fornitura di servizi e acquisto di beni per le attività inerenti la comunicazione e educazione e adempimenti correlati

Il sistema di gestione e controllo è comunque specificato all'interno del presente documento che ne descrive e disegna i processi e le procedure tecniche eventuali; ma anche attraverso AUDIT periodici annuali, che verificano l'applicazione dei processi stessi e mantengono memoria delle evidenze esaminate a riprova della validità del Sistema. All'interno del suo sistema gestionale l' Ente Regionale RomaNatura ha implementato il seguente documento specifico per la gestione dei processi definiti determine

- **Documento 1**- Diagrammi di flusso della gestione dei processi operativi definiti determine:
  - Flusso Determina Direttore;
  - Flusso Determina Dirigente;
  - Flusso Determina Rup Direttore;
  - Flusso Determina Rup Dirigente.

Questa documentazione, allegata al presente disciplinare,descrive dettagliatamente architettura, obblighi e responsabilità del sistema operativo dell'Ente Regionale RomaNatura.

13 Figure, Posizioni e compiti del Sistema della Privacy

L'Ente Regionale RomaNatura ha stabilito le figure, posizioni e compiti del sistema privacy tenendo conto del principio secondo cui la tutela dei dati personali deve porre l'utente al centro del proprio sistema di controllo, obbligando chi detiene il dato ad una tutela effettiva da un punto di vista sostanziale e non solo formale.

Il Regolamento europeo per la protezione dei dati personali impone al Titolare del Trattamento l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti. L'articolo 25, in particolare, introduce il principio di privacy by design e privacy by default, un approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, cioè fin dal momento dell'inizio dell'attività progettuale, gli strumenti a tutela dei dati personali.

13.1 Data Protection Officer – DPO/RPD – Responsabile Protezione dei Dati

L'Ente Regionale RomaNatura ha deciso, seguendo le indicazioni del Regolamento 679/2016, di introdurre nel proprio sistema Privacy il Data Protection Officer o, in Italiano, il Responsabile Protezione Dati, poiché essendo Ente Pubblico, l'Ente Regionale RomaNatura ha l'obbligo di tale nomina.

Il DPO:

- ha BUDGET DI SPESA AUTONOMO per assolvere ai compiti, accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica
- NON DEVE RICEVERE ISTRUZIONI (interferenze) circa l'adempimento dei propri compiti
- non può essere penalizzato o rimosso per l'adempimento dei propri compiti
- riferisce direttamente al vertice gerarchico del Titolare o del Responsabile del trattamento
- è la figura di contatto per tutti gli interessati relativamente alle questioni legate al trattamento dei dati personali e all'esercizio dei loro diritti
- è tenuto al Segreto o alla riservatezza

Ed ha i seguenti compiti:

- INFORMARE e fornire consulenza al Titolare o Responsabile del trattamento nonché ai dipendenti (incaricati) che eseguono il trattamento
- SORVEGLIARE l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri nonché delle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei

dati personali, compresi sia l'attribuzione delle responsabilità che la sensibilizzazione e ~~la~~ formazione del personale coinvolto
- FORNIRE, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati;
- SORVEGLIARE lo svolgimento delle attività
- COOPERARE con l'Autorità di Controllo e fungere da punto di contatto per questioni connesse al trattamento, tra cui la consultazione preventiva (ex verifica preliminare).

13.2 Responsabile al trattamento dei dati

È la figura obbligatoria al Sistema nel caso in cui un trattamento debba essere effettuato per conto del Titolare del Trattamento; a lui spetta il compito di:

- promuovere lo sviluppo ed il mantenimento dei programmi di sicurezza in essere nel presente disciplinare contenente tutte le indicazioni cogenti relative alla sicurezza dei dati personali;
- informare il titolare sulle non corrispondenze con le norme di sicurezza e sugli eventuali incidenti;
- promuovere un programma continuo di addestramento degli incaricati al trattamento e mantenere attivo un programma di controllo, sorveglianza e monitoraggio della corrispondenza con le regole di sicurezza;
- promuovere e garantire l'esecuzione del programma di Audit.

Questa figura deve essere consapevole circa la natura e la finalità del trattamento,il tipo di dati personali e le categorie di interessati,gli obblighi e i diritti del titolare del trattamento e le funzioni attribuite al ruolo.

13.3 Responsabile della gestione del sistema informatico ed Amministratore di Sistema

Il sistema di sicurezza informatica è il mezzo di tutela centrale del sistema privacy dell'Ente Regionale RomaNatura. Si ispira ad un approccio basato sulla valutazione del rischio (*risk based approach*), con il quale si riesce a determinare la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, della frequenza,del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. Nel capitolo15 del presente disciplinare l'Ente Regionale RomaNatura descrive dettagliatamente la valutazione del rischio e tutti i concetti ad essa correlati. Tale valutazione del rischio si connette con quello definito anche nel modello di Organizzazione,Gestione e Controllo ex D.lgs 231/2001 redatto dalla Regione Lazio.

Il responsabile alla gestione del sistema informatico è quindi una figura, alla quale spettano diversi compiti, sia in accordo al Reg. 679/2016,sia in ottemperanza al provvedimento del Garante della Privacy su "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" del 27 novembre 2008 e successive modifiche del 25 giugno 2009.

Obblighi e responsabilità del Responsabile della gestione del Sistema sono di seguito riportati:

- promuovere e sviluppare i programmi di sicurezza contenuti nel presente Disciplinare ed indicati nel GDPR; informare il titolare del trattamento sulle non corrispondenze e sugli eventuali incidenti;
- promuovere lo svolgimento di un costante e continuo programma di addestramento degli incaricati al trattamento e mantenere attivo un programma di controllo, sorveglianza e monitoraggio della corrispondenza con le regole di sicurezza;
- promuovere e garantire l'esecuzione del programma di audit; garantire il funzionamento di tutti i dispositivi elettronici; degli strumenti, dei sistemi operativi, dei software, con particolare attenzione ai sistemi Antivirus, Firewall, al sistema di back-up, al sistema del ripristino dei dati, alle reti, al sistema degli accessi;
- registrare i log degli accessi degli incaricati all'amministrazione del Sistema informatico ed in generale ai sistemi informativi;

- garantire che i log acquisiti siano integri, completi e inalterabili; conservare i log acquisiti per 6 mesi dalla loro registrazione.

Inoltre svolge le attività utili alla gestione del sistema informatico; … Omissis ….

13.4 Incaricati al trattamento

Sono nominati dal Responsabile del Trattamento per iscritto e devono:

- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Disciplinare e secondo le direttive del Responsabile al trattamento dei dati;
- rispettare e far rispettare le normative di sicurezza e le misure per la protezione dei dati personali;
- segnalare al DPO eventuali anomalie o comportamenti pregiudizievoli sul trattamento dei dati;
- informare il DPO in caso di incidenti di sicurezza che coinvolgano i dati personali.

Il custode delle credenziali e delle password

….Omissis …..

Outsourcer

….. Omissis ….

Soggetti autorizzati all'accesso ai locali fuori dall'orario di lavoro

Sono quei soggetti (dipendenti, collaboratori, operatori di ditte esterne) che hanno ricevuto autorizzazione scritta dall'Ente ad accedere nelle sedi dell'Ente stesso, fuori dall'orario di lavoro.

14 Strumenti

Con il termine strumento si indicano gli elaborati, i programmi per elaboratori, qualunque dispositivo elettronico automatizzato o qualsiasi contenitore o mezzo impiegato per effettuare il trattamento dati.

….. Omissis …..

15 Rischi

Sono situazioni o comportamenti che possano generare un pericolo per i dati personali e/o sensibili. Per meglio valutare l'entità e le azioni da intraprendere il rischio prevede diversi livelli di soglia: lieve, medio, grave e gravissimo.

L'Ente Regionale RomaNatura ha implementato un sistema di gestione aziendale in generale e in particolare merito rispetto alle disposizioni sulla Privacy, basato sul risk based thinking ovvero su un approccio pratico e immediato per identificare i fattori di rischio e di opportunitàil prima possibile, e gestirli in modo preventivo. Agendo in questo modo l'approccio diventa proattivo, al fine di ridurre gli effetti indesiderati attraverso l'identificazione dei fattori che potrebbero fare deviare i processi e il sistema di gestione dai risultati pianificati. Tutto questo viene attuato mettendo in atto misure e controlli per minimizzare preventivamente gli effetti negativi e massimizzare le opportunità, quando esse si presentano.

In accordo con l'articolo 25 del Reg.679/2016l'Ente Regionale RomaNatura ha fatto suoi i concetti di *privacy by design*e *privacy bydefault*, implementandoli nel suo sistema privacy. Si riporta di seguito i capi essenziali dell'articolo 25:

….. Omissis ……

16 Procedure di autenticazione

L'Ente Regionale RomaNatura ha implementato le procedure di seguito riportate, per la gestione degli accessi logici, intesi come utilizzazioni della rete o del computer in locale da parte di un qualsiasi utente, per lo svolgimento dell'attività lavorativa quotidiana.

…..Omissis ……

Macchine - Accesso alle procedure applicative specifiche

….. Omissis …..

CED - Gestione degli accessi logici.

…. Omissis ….

La postazione sistemistica

Consente di effettuare operazioni sistemistiche particolari, quali installazione e disinstallazione di unità, modifica degli applicativi, ecc. Le persone alle quali è consentito accedere e alle quali è assegnato un sistema di credenziali di autenticazione sono individuate dall'Amministratore di Sistema

…. Omissis ….

17 Misure a tutela della Privacy

A tutela della privacy dei propri dati sono previste specifiche misure di protezione e sicurezza: in caso di violazione della privacy i principali strumenti a disposizione sono:

- La Segnalazione;
- Il Reclamo;
- Il Ricorso.

Tutti e tre i tipi di istanza vengono proposti al Garante della Privacy.

La segnalazione: è un atto (generico e non circostanziato come il reclamo) finalizzato a sollecitare l'esercizio dell'attività di controllo da parte del Garante. La segnalazione è gratuita, non presenta particolari formalità e deve essere inviata al Garante. Ad una o più segnalazioni possono seguire un'istruttoria preliminare ed un procedimento amministrativo nel quale possono essere adottati vari provvedimenti (anche prima della definizione del procedimento).

Il reclamo è un atto (che non prevede particolari formalità) con il quale l'interessato denuncia (dietro il pagamento di una somma di euro 150 a titolo di diritti di segreteria) al Garante una violazione della disciplina in materia di protezione dei dati personali.

Può essere proposto:

- quando non si è ottenuta una tutela soddisfacente dei propri diritti;
- quando si vuole promuovere una decisione del garante su una questione di sua competenza.

Il reclamo deve contenere l'indicazione:

- dei fatti e delle circostanze su cui si fonda;
- delle disposizioni che si presumono violate;
- delle misure richieste;
- degli estremi identificativi del titolare, del responsabile (se conosciuto) e del richiedente.

A seguito della ricezione del reclamo vi sarà un'istruttoria preliminare che valuterà la fondatezza del reclamo; a seguito di ciò (in caso di ricorso fondato) il Garante definirà il procedimento prescrivendo una delle seguenti misure:

- invitare il titolare ad effettuare il blocco spontaneo;
- prescrivere al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;

- disporre il blocco o vietare, in tutto o in parte, il trattamento che risulta illecito (o non corretto) anche per effetto della mancata adozione delle misure necessarie oppure quando, in considerazione della natura dei dati o delle modalità del trattamento, vi è il concreto rischio di arrecare un danno ad uno o più interessati.

Il ricorso al Garante è un atto formale, che deve essere presentato rispettando particolari formalità e unicamente nei seguenti casi:

- in caso di risposta tardiva (quindi oltre i 15 o 30 giorni dalla richiesta) o non soddisfacente da parte del titolare del trattamento dei dati o del responsabile (se designato);
- se il decorso dei termini relativi al riscontro dell'istanza esporrebbe l'interessato ad un pregiudizio imminente ed irreparabile.

Il ricorso non è gratuito: anche in questo caso (come per il reclamo) è pari a 150 euro a titolo di diritti di segreteria.

Il ricorso deve contenere:

- gli estremi identificativi del ricorrente, dell'eventuale procuratore speciale, del titolare e (ove conosciuto) del responsabile eventualmente designato;
- la data dell'istanza presentata al titolare (o al responsabile), oppure la data in cui si è verificato il danno imminente ed irreparabile;
- gli elementi posti a fondamento della domanda;
- il provvedimento richiesto al Garante;
- il domicilio eletto ai fini del procedimento.

Il Garante, se ritiene fondato il ricorso, può ordinare la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto (cosiddetto silenzio – diniego). Contro il provvedimento (espresso o tacito) del Garante è possibile proporre ricorso dinanzi al Tribunale del luogo nel quale risiede il Titolare del trattamento.

17.1 Violazione e Reati

Per meglio garantire l'osservanza delle disposizioni del presente disciplinare in merito alla protezione e tutela del trattamento dei dati personali, L'Ente Regionale RomaNatura ha voluto riportare di seguito i diversi tipi di reati e le sanzioni previste dal nuovo regolamento 679/2016 per eventuali inosservanze da parte di responsabili e/o incaricati del trattamento.

Ai sensi dell'art. 83 del nuovo regolamento 679/2016, sono previste sanzioni (c.d. multe) che, devono avere carattere di effettività, proporzionalità e dissuasività.

Le sanzioni amministrative riportate nell'elenco che segue, possono essere integrative, oppure completamente sostitutive. Si distinguono in sanzioni di carattere economico o amministrative:

La decisione sull'applicazione delle sanzioni spetta all'autorità di controllo (in Italia: l'Autorità Garante per la Protezione dei Dati Personali), che, nella valutazione, tiene conto delle circostanze del singolo caso, ossia:

– della natura, gravità e durata della violazione
– del carattere doloso o colposo della violazione

– delle misure adottate per attenuare il danno subito dagli interessati
– delle eventuali precedenti violazioni commesse dal titolare del trattamento
– del grado di cooperazione con l'autorità di controllo
– degli eventuali altri fattori aggravanti o attenuanti

17.2 Sanzioni di carattere economico

….. Omissis …..

17.3 Sanzioni correttive amministrative

Le sanzioni sono connesse ai poteri dell'Autorità di controllo e consistono nel:

……. Omissis …..

17.4 Risarcimento del danno

L'articolo 82 del Regolamento Europeo 679/2016 prevede che "Chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento".

Dunque, in aggiunta al risarcimento dei danni patrimoniali arrecati, la violazione delle prescrizioni relative alle modalità del trattamento e ai requisiti dei dati fa nascere in capo all'autore l'obbligo di risarcire il danno morale arrecato all'interessato, indipendentemente dalla consumazione di un reato.

18 Architettura della gestione del dato

Elenco dei trattamenti dei dati personali

… Omissis …..

Distribuzione dei compiti e delle Responsabilità

Il Diretto dell'Ente Regionale RomaNatura, quale coordinatore generale e responsabile della correttezza amministrativa ha individuato e quindi conferito con lettera allegata in copia al presente documento, l'Incarico di Responsabile al Trattamento dei Dati a:

Denominazione del Responsabile al Trattamento	Data Assunzione Incarico	Data Scadenza Incarico	Data Formazione
Dott. Danilo Casciani – Responsabile Generale del Trattamento Via Gomenizza, 81 - ROMA	07/04/2017	N/A	Maggio/settembre 2018

Dott. Vincenzo Frangione – Responsabile del Trattamento per il settore Amministrativo Via Gomenizza, 81 - ROMA	16/11/2016	N/A	Maggio/settembre 2018
Dott. Cosimo Marco Calò – Responsabile del Trattamento per il settore Tecnico e Urbanistico Via Gomenizza, 81 - ROMA	16/08/2016	N/A	Maggio/settembre 2018
D.ssa Giacomini Antonella – Responsabile del trattamento per il settore ICT Via Gomenizza,81 – ROMA	16/04/2007	N/A	Maggio/settembre 2018
Responsabile esterno della gestione dei dati personali" la Soc. APKAPPA Smart Technologies del gruppo Maggioli che gestisce, relativamente ad un contratto per fornitura di software gestionale e gestione in cloud, il trattamento dei dati dell'Ente RomaNatura.	Contratto fornitura dal 2017	N/A	Maggio/settembre 2018

Questi ultimi sono responsabili dei seguenti trattamenti:

---- Omissis …..

19 Analisi dei rischi che incombono sui dati

Di seguito si riporta l'elenco, esemplificativo e non esaustivo, dei principali rischi prevedibili, classificati in base alla fonte ed alle possibili conseguenze:

Eventi relativi al contesto: accessi non autorizzati a locali/reparti di accesso ristretto, asportazione e furto di strumenti contenenti dati, eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria, guasto ai sistemi complementari (impianto elettrico, climatizzazione), errori umani nella gestione della sicurezza fisica.

Eventi relativi ai comportamenti degli operatori: furto di credenziali di autenticazione , carenza di consapevolezza, disattenzione o incuria, trattamenti non consentiti, errore materiale, distruzione o perdita dati anche accidentale, comportamenti sleali o fraudolenti, trattamenti non conformi alle finalità.

Eventi relativi agli strumenti: malfunzionamenti dovuti a: azione di virus informatici o di codici malefici, malfunzionamento, indisponibilità o degrado degli strumenti, accessi esterni non autorizzati, intercettazione di informazioni in rete, guasti, eventi naturali quali terremoti, allagamenti, incendi, blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica, a sabotaggi, furti.

Analisi dei rischi relativi ai luoghi

Rischi/Evento	Eventi Naturali
Valutazione/gravità	Molto bassa
Descrizione Impatto	Eventi Naturali
Riferimento alle misure	Progettazione immobile
Luoghi	Sede

Rischi/Evento	Possibili Intrusioni
Valutazione/gravità	Molto bassa
Descrizione Impatto	Possibili Intrusioni non autorizzate ai locali
Riferimento alle misure	Sistema di allarme Istituto di vigilanza privata

Luoghi	Sede– CED

Rischi/Evento	Furti
Valutazione/gravità	Medio/bassa
Descrizione Impatto	software, hardware
Riferimento alle misure	Antifurto Accesso controllato da Istituto di vigilanza privata
Luoghi	Sede

Rischi/Evento	Incendi
Valutazione/gravità	Molto bassa
Descrizione Impatto	Eventi Naturali, fortuiti, dolosi
Riferimento alle misure	Identificate nel Documento di Prevenzione e Protezione Dlgs 81/08
Luoghi	Sede

Analisi dei rischi relativi ai software

Rischi/Evento	Bug
Valutazione/gravità	Elevata
Descrizione Impatto	Bug che minacciano l'integrità dei dati e/o lo stesso applicativo
Riferimento alle misure	L'analisi e la valutazione dei rischi per la sicurezza della infrastruttura IT individuandone le vulnerabilità, in termini di "bug" dei software installati, e di errate configurazioni dei sistemi operativi piuttosto che degli applicativi. Per quanto riguarda i sistemi operativi nonché il software di terze parti installati presso l'azienda, si fa riferimento ai sistemi di verifica e log proprietari con specifici eventuali aggiornamenti o service pack installati. Per quanto riguarda i software sviluppati internamente, attraverso le attività di tracciamento del ciclo di vita del software, possono essere misurati ed individuati i punti deboli di quanto prodotto in modo da assegnare una priorità ai rischi e fornire report con diversi livelli di dettaglio e con istruzioni step-by-step per l`eliminazione delle eventuali vulnerabilità.
Luoghi	Sede

Rischi/Evento	Virus/Malware
Valutazione/gravità	Elevata
Descrizione Impatto	Virus informatico trasmesso tramite posta elettronica, connessione ad internet, CD/DVD/USB drive infetti, attacchi dall'interno della rete locale LAN o VPN
Riferimento alle misure	*Verifica giornaliera dei log di sistema e dei prodotti antivirus centralizzati installati su ogni Server e workstation.* *Verifica dell'aggiornamento quotidiano delle definizioni dei virus.* *Verifica dell'aggiornamento periodico di eventuali patch di sicurezza di sistema operativo (server e workstation).*

	Scansione settimanale completa automatica e centralizzata su tutti i client e server della rete.
Luoghi	Sede

Rischi/Evento	Spyware
Valutazione/gravità	Elevata
Descrizione Impatto	Aggressione da software in grado di trasmettere informazioni riservate attraverso intrusioni software
Riferimento alle misure	*Verifica giornaliera dei log di sistema e dei prodotti antivirus centralizzati installati su ogni Server e workstation.* *Verifica dell'aggiornamento quotidiano delle definizioni dei virus* *Verifica dell'aggiornamento periodico di eventuali patch di sicurezza di sistema operativo (server e workstation).* *Scansione settimanale completa automatica e centralizzata su tutti i client e server della rete.*
Luoghi	Sede

Rischi/Evento	Trojan
Valutazione/gravità	Elevato
Descrizione Impatto	Applicativi che sfruttano particolari vulnerabilità del sistema operativo, o particolari porte del protocollo di comunicazione per danneggiare l'utente sotto attacco.
Riferimento alle misure	*Verifica giornaliera dei log di sistema e dei prodotti antivirus centralizzati installati su ogni Server e workstation.* *Verifica dell'aggiornamento quotidiano delle definizioni dei virus* *Verifica dell'aggiornamento periodico di eventuali patch di sicurezza di sistema operativo per server e workstation.* *Scansione settimanale completa su tutti i client e server della rete, automatica, centralizzata.*
Luoghi	Sede

Rischi/Evento	Worm
Valutazione/gravità	Elevato
Descrizione Impatto	Applicativi che danneggiano i computer, rubano rubriche, account e si auto replicano
Riferimento alle misure	*Verifica giornaliera dei log di sistema e dei prodotti antivirus centralizzati installati su ogni Server e workstation.* *Verifica dell'aggiornamento quotidiano delle definizioni dei virus* *Verifica dell'aggiornamento periodico di eventuali patch di sicurezza di sistema operativo (server e workstation).*

	Scansione settimanale completa automatica e centralizzata su tutti i client e server della rete.
Luoghi	Sede

Rischi/Evento	Backdoor
Valutazione/gravità	Elevata
Descrizione Impatto	Applicativi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione
Riferimento alle misure	*Verifica giornaliera dei log di sistema e dei prodotti antivirus centralizzati installati su ogni Server e workstation.* *Verifica dell'aggiornamento quotidiano delle definizioni dei virus* *Verifica dell'aggiornamento periodico di eventuali patch di sicurezza di sistema operativo (server e workstation).* *Scansione settimanale completa automatica e centralizzata su tutti i client e server della rete.*
Luoghi	Sede

Rischi/Evento	Hijacker
Valutazione/gravità	Elevata
Descrizione Impatto	Applicativi che si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine Web indesiderate
Riferimento alle misure	*Verifica giornaliera dei log di sistema e dei prodotti antivirus centralizzati installati su ogni Server e workstation.* *Verifica dell'aggiornamento quotidiano delle definizioni dei virus* *Verifica dell'aggiornamento periodico di eventuali patch di sicurezza di sistema operativo (server e workstation).* *Scansione settimanale completa automatica e centralizzata su tutti i client e server della rete.*
Luoghi	Sede

Rischi/Evento	Adware
Valutazione/gravità	Elevata
Descrizione Impatto	Applicativi che causano danni e rallentamenti del pc nonché rischi per la privacy comunicando le abitudini di navigazione ad un server remoto
Riferimento alle misure	*Verifica giornaliera dei log di sistema e dei prodotti antivirus centralizzati installati su ogni Server e workstation.* *Verifica dell'aggiornamento quotidiano delle definizioni dei virus* *Verifica dell'aggiornamento periodico di eventuali patch di sicurezza di sistema operativo (server e workstation).*

	Scansione settimanale completa automatica e centralizzata su tutti i client e server della rete.
Luoghi	Sede

Rischi/Evento	Keylogger
Valutazione/gravità	Elevata
Descrizione Impatto	Applicativi in grado di registrare tutto ciò che un utente digita su una tastiera rendendo possibile il furto di password o di dati
Riferimento alle misure	*Verifica giornaliera dei log di sistema e dei prodotti antivirus centralizzati installati su ogni Server e workstation.* *Verifica dell'aggiornamento quotidiano delle definizioni dei virus* *Verifica dell'aggiornamento periodico di eventuali patch di sicurezza di sistema operativo (server e workstation).* *Scansione settimanale completa automatica e centralizzata su tutti i client e server della rete.*
Luoghi	Sede

Analisi dei rischi relativi agli strumenti hardware

Rischi/Evento	Uso non autorizzato Hardware
Valutazione/gravità	Medio
Descrizione Impatto	Uso non autorizzato dell'hardware consentito dall'utilizzatore, o per poca attenzione dello stesso
Riferimento alle misure	• Chiave (accesso al locale) • Password (accesso al PDL)
Luoghi	Sede

Rischi/Evento	Guasto
Valutazione/gravità	Basso
Descrizione Impatto	Guasto degli apparecchi dovuti a cause varie
Riferimento alle misure	Manutenzione tramite contratto triennale di manutenzione fornito dalla casa produttrice con intervento on site nelle 24 ore
Luoghi	Sede

Rischi/Evento	Eventi naturali
Valutazione/gravità	Basso
Descrizione Impatto	Eventi naturali
Riferimento alle misure	Ridondanza in duplicazione del CED e backup + piattaforma virtuale di replica a caldo dei server in semi continuità operativa
Luoghi	Server

Rischi/Evento	Furti
Valutazione/gravità	Medio/bassa
Descrizione Impatto	Progetti, software, hardware

Riferimento alle misure	Antifurto Accesso controllato da Istituto di vigilanza privata
Luoghi	Sede

Analisi dei rischi relativi alle banche dati

….. Omissis …..

20 Piano di Valutazione d'impatto sui Dati Personali

Il nuovo regolamento Europeo introduce il **DPIA (Data Protection Impact Assessment)** ovvero un Piano di Valutazione d'impatto sui Dati Personali che deve essere adottato dai Titolari/Responsabili che trattano dati che, per natura, scopo, finalità, presentano specifici rischi per i diritti fondamentali degli interessati nonché le libertà personali.

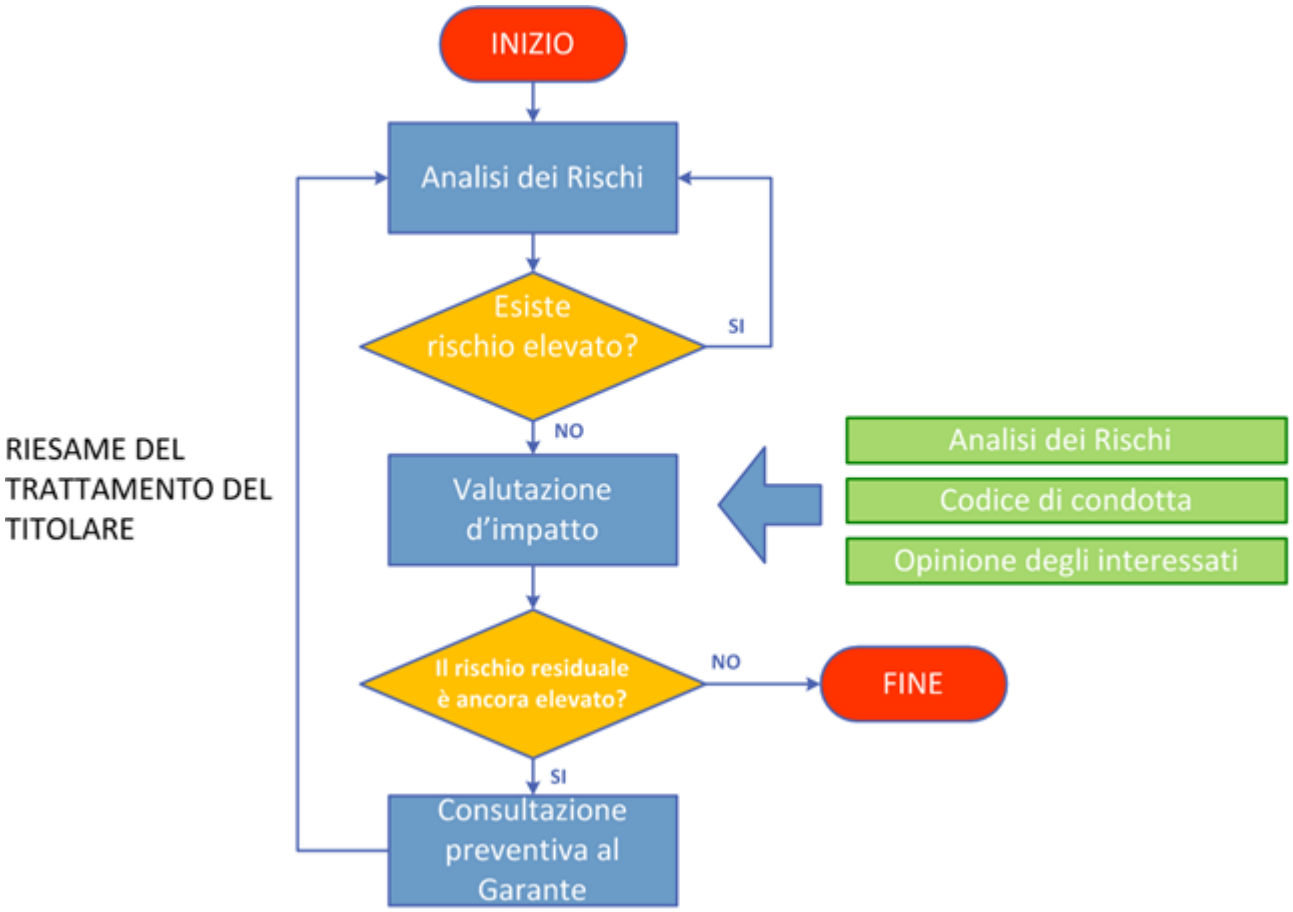


Diagramma di flusso del Piano di Valutazione d'impatto sui Dati Personali

Il DPIA non si limita alle considerazioni tecniche dei sistemi informatici, ma si applica ai sistemi informativi in modo completo, da tali sistemi a persone, documenti cartacei, organizzazione e locali.

Infine, il DPIA aiuta a dimostrare l'attuazione dei principi di riservatezza in modo che gli interessati mantengano il controllo dei propri dati personali.

L'Ente Regionale RomaNatura ritiene che non sia necessario eseguire un DPIA per ogni trattamento gestito ma sfruttare quanto disposto dall'articolo 35 del GDPR che afferma che "*una singola valutazione può affrontare una serie di operazioni di trattamento simili che presentano rischi simili elevati*".

Pur gestendo trattamenti diversi, l'Ente Regionale RomaNatura considera che sia ragionevole ed economico effettuare una valutazione d'impatto su più trattamenti contemporaneamente che siano simili in termini di rischi presentati, avendone adeguatamente considerato la specifica natura, portata, contesto e finalità.

…… Omissis …..

20.1 Valutazione di impatto sulla protezione dei dati

Le funzioni operative e di organizzazione delle attività dell'Ente hanno l'onere di effettuare una preliminare valutazione di impatto privacy sui trattamenti effettuati quando gli stessi possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Tale valutazione, consente di considerare, prima che il trattamento venga posto in essere, il rischio, ossia l'incidenza, delle attività poste in essere dal Titolare sui dati personali.

Il DPIA ha quindi l'obiettivo di identificare in anticipo i possibili rischi che possono derivare dalle attività di trattamento svolte dall'Ente Regionale RomaNatura e definire le misure di sicurezza tecniche ed organizzative adeguate ai livelli di rischio rilevati. Il *Data Protection Impact Assessment* applicato ai nuovi trattamenti è da considerarsi parte integrante del processo di Privacy by Design. Tuttavia, il *Data Protection Impact Assessment* non si esaurisce nel processo di Privacy by Design, ma è da intendersi come un processo continuativo che deve essere condotto iterativamente sul trattamento ogni qualvolta questo subisca una variazione significativa.

Il responsabile del progetto procede quindi a raccogliere tutti i dati e le informazioni necessarie per poter eseguire la valutazione di impatto sulla protezione dei dati.

Qualora lo ritenga necessario procede a coinvolgere le altre funzioni al fine di reperire tutte le informazioni di cui necessita. Al fine di valutare il livello di rischio per ciascuno scenario procedealla compilazione del modello di valutazione d'impatto sulla protezione dei dati (foglio Excel allegato).

20.2 Misurazione del rischio inerente

Il modello di valutazione d'impatto sulla protezione dei dati personali partendo dagli scenari di rischio privacy definisce i potenziali eventi. Determinati i potenziali eventi si procede alla valutazione del livello di rischio effettuata mediante la valutazione dei seguenti elementi:

- **Impatto**. Impatto che un errato trattamento dei dati potrebbe avere nei confronti di un soggetto interessato;
- **Probabilità.** Probabilità che un errato trattamento dei dati generi un particolare impatto sui diritti e sulle libertà delle persone.

Il livello di probabilità sarà definito dal responsabile di progetto sulla base dell'effettiva operatività prevista per il progetto oggetto di analisi.

….. Omissis ……

21 Misure in essere e da adottare

In ottemperanza al nuovo regolamento 679/2016 i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

In aggiunta al rispetto dei predetti obblighi di sicurezza generali, l'Ente Regionale RomaNatura deve rispettare le prescrizioni in materia di misure minime di sicurezza, distinte in base alla modalità con cui viene effettuato il trattamento con strumenti elettronici o meno.

Per il trattamento di dati personali effettuato con strumenti elettronici (di cui alla presente sezione) l'Ente Regionale RomaNatura ha adottato le seguenti misure:

…..Omissis …….

Tali misure devono essere adottate con modalità tecniche che non scendano al di sotto dei limiti fissati dalla normativa vigente relativi, in particolare, all'adozione di idonei sistemi di autenticazione informatica e di autorizzazione (la cui applicazione è esclusa solo per i trattamenti dei dati personali destinati alla diffusione), in aggiunta alle altre tassative misure di sicurezza.

Sistema di autenticazione informatica

….. Omissis …..

Descrizione dei sistemi di protezione degli strumenti elettronici: antivirus e relativo aggiornamento

…… Omissis …..

Descrizione delle procedure per la protezione dei dati da perdita improvvisa

……. Omissis …….

Gestione delle procedure di back up

….. Omissis …..

Elenco delle misure in essere e da adottare

Tutte le misure di seguito elencate seguono la seguente verifica da check-list di sistema privacy:

…… Omissis ……

22 Videosorveglianza

Non Applicabile

23 Criteri e modalità di recupero della disponibilità dei dati

….. Omissis …….

24 Formazione dei responsabili e degli incaricati al trattamento dei dati

…… Omissis …..

25 Misure di tutela e garanzia

Misure di sicurezza adottate presso soggetti esterni

Il Titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere all'esecuzione, riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Trasferimento dei dati personali presso Paesi Terzi

Non applicabile

26 Misure aggiuntive riservate al trattamento dei dati personali sensibili e giuridici.

…… Omissis …..

Istruzioni organizzative e tecniche per i supporti rimovibili

L'Ente Regionale RomaNatura prevede che siano impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

In particolare i supporti rimovibili e le copie di back-up sono conservate in luoghi protetti e in contenitori chiusi a chiave.

Supporti rimovibili contenenti dati sensibili non utilizzati

…. Omissis ……

Recupero di supporti rimovibili contenenti dati sensibili non utilizzati

…. Omissis …..

Sistema di utilizzo dei dati sensibili

…..Omissis ……

27 Elenco dei luoghi in cui verranno trattati i dati

Nelle tabelle seguenti sono riportati in modo schematico i luoghi in cui sono trattati i dati con annesse responsabilità, caratteristiche e sistemi di protezione attivi.

….. Omissis …….

28 Elenco delle banche dati utilizzate nei diversi trattamenti

….. Omissis ……

Tabella riassuntiva di riferimento alla normativa:
Trattamento di dati idonei a rivelare lo stato di salute,situazione legale e giudiziaria
Categorie di dati: dati idonei a rivelare lo stato di disabilità; dati idonei a rivelare lo stato di salute e la situazione legale/giudiziaria.
Categorie a cui i dati si riferiscono: Lavoratori e/o collaboratori – soggetti per i quali è stata effettuata Determina, soggetti nei confronti dei quali è stata comminata Ammenda
Finalità: Gestione amministrativa - giudiziaria
Modalità di trattamento: raccolta di dati al fine di trattamento da parte di terzi

Ambiti di comunicazione: Persone fisiche, società di persone, imprese individuali.
Dati sul luogo della custodia: vedi riferimenti sopra riportati.

29 Elenco dei software utilizzati nei diversi trattamenti

….. Omissis ……

30 Informativa e formula di acquisizione al consenso al trattamento dei dati personali

Il nuovo regolamento 679/2016 insieme a specifici provvedimenti generali dell'Autorità Garante prevedono *informativa* e *consenso* come garanzie ed accorgimenti da osservare per la protezione del dato.

I predetti accorgimenti/garanzie, possono comportare, se non sono rispettati, l'inutilizzabilità dei dati trattati.

Una maggiore attenzione deve essere prestata all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati in caso di:

- acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati;
- scambio di corrispondenza, specie per via telematica;
- esercizio contiguo di attività autonome all'interno di uno studio;
- utilizzo di dati di cui è dubbio l'impiego lecito, anche per effetto del ricorso a tecniche invasive;
- utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti (tabulati di flussi telefonici e informatici, consulenze tecniche e perizie, relazioni redatte da investigatori privati);
- custodia di materiale documentato, ma non utilizzato in un procedimento e ricerche su banche dati a uso interno, specie se consultabili anche telematicamente da uffici adibiti allo stesso titolare del trattamento, ma situati altrove;
- acquisizione di dati e documenti da terzi, verificando che si abbia titolo per ottenerli;
- conservazione di atti relativi ad affari definiti.

In merito a quest'ultimo aspetto si ricorda che i dati personali sono conservati dall'Ente Regionale RomaNatura, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti.

A tal fine, anche mediante controlli periodici, deve essere verificata la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto agli incarichi in corso, da instaurare o cessare, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

30.1 Informativa

L'informativa è l'obbligo dei Responsabili del trattamento di informare preventivamente l'interessato, al fine di renderlo edotto dei suoi diritti previsti dal Regolamento circa le finalità di seguito riportate:

- le finalità e le modalità del trattamento dei dati,
- la natura obbligatoria o facoltativa del conferimento dei dati,

- le conseguenze di un eventuale rifiuto di rispondere,
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati,
- il diritto di accesso dell'interessato ed i diritti connessi,
- le generalità del titolare ed eventualmente del responsabile.

L'informativa, va resa al momento della raccolta dei dati; se detti dati non venissero raccolti presso l'Ente, ma trasmessi da un terzo autorizzato, l'informativa andrà inoltrata all'atto della registrazione; in ogni caso non oltre la prima comunicazione a terzi dei medesimi, necessaria in virtù dello specifico conferimento.

30.2 Consenso

L'Informativa deve essere comunicata all'interessato anche per permettere a quest'ultimo di prestare validamente il proprio consenso. Oltre a dover essere esplicito, infatti, "il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni in accordo con l'articolo 13 (informativa) del nuovo regolamento.

In generale, a prescindere da specifiche normative, la tutela accordata dall'ordinamento giuridico alla propria immagine, al proprio nome, alla propria identità, al segreto epistolare e telefonico impone di ritenere, per analogia, vietata la diffusione senza consenso di notizie della vita privata la cui pubblica conoscenza non sia di alcuna utilità sociale.

Sicuramente negli ultimi tempi il requisito del consenso ha assunto un significato particolare in quanto con l'avvento delle tecnologie informatiche il "right to privacy" ha acquistato un nuovo significato ed una nuova ampiezza, che non poteva avere un secolo fa.

Il consenso del cliente non va richiesto per adempiere a obblighi di legge e non occorre, altresì, per i dati anche di natura sensibile utilizzati per perseguire finalità di difesa di un diritto anche mediante investigazioni difensive.

Occorre peraltro avere cura di rispettare, se si tratta di dati idonei a rivelare lo stato di salute e la vita sessuale, il principio del "pari rango", il quale giustifica il loro trattamento quando il diritto che si intende tutelare, anche derivante da atto o fatto illecito, è "di rango pari" a quello dell'interessato, ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile.

Il trattamento dei dati sensibili può essere effettuato ai soli fini dell'espletamento di un incarico che rientri tra quelli che l'Ente può eseguire in base alle proprie competenze.

In accordo con la cogenza di privacy prevista L'Ente Regionale RomaNaturaha implementato i propri moduli tipo (lettera al consenso dei dati), allegati al presente GDPR.

31 Documento di verifica dell'applicazione delle misure (check-list)

Il presente documento garantisce l'evidenza oggettiva dell'attuazione delle misure adottate.

….. Omissis ……

32 Piano di verifica dei controlli a scadenza inferiore a sei mesi

Il presente documento garantisce l'evidenza oggettiva dell'attuazione sulle misure adottate in materia di privacy dall'Ente Regionale RomaNatura. La verifica è stata volutamente resa più frequente rispetto agli obblighi previsti dalla normativa al fine di preservare il titolare al trattamento dei dati oltre che da sanzioni di natura penale (su cui sarebbero sufficienti le misure minime) anche le sanzioni da eventuali abusi in sede

civile. La maggior frequenza dei controlli garantisce una minor probabilità di abuso ed in ogni caso una dimostrazione di maggior diligenza nel preservare i dati.

La presente misura,

…… Omissis

riportata tra le misure minime previste dal Regolamento sulla Privacy, potrà essere verificata attraverso una tabella o attraverso un sistema di notifica automatica (sistema scelto da RomaNatura) che il software potrà gestire automaticamente per l'incaricato preposto alla verifica di funzionamento del sistema back-up. Inoltre il GDPR riporta la necessità di controllare il funzionamento del sistema di aggiornamento del software antivirus.

La presente misura,

…. Omissis …..

riportata tra le misure minime previste dal Regolamento sulla privacy,potrà essere verificata attraverso la seguente tabella ad intervalli mensili dall'incaricato preposto alla verifica di funzionamento del sistema di ripristino dei dati affinché in caso di necessità, (che sarà garantita entro sette giorni) se ne accerti il funzionamento.

…. Omissis …..

33 Verbale di verifica variazione password

L'Ente Regionale RomaNatura prevede la verifica delle variazioni password con autenticazione AD come descritto in precedenza, pertanto la redazione di un *verbale di verifica*risulta non applicabile.

34 Allegati al presente disciplinare

Al presente GDPR sono allegati 12 documenti, e precisamente:

1. Lettera di nomina a Responsabile esterno al trattamento dei dati
2. Lettera di nomina a Responsabile Interno al trattamento dei dati
3. Lettera di nomina a incaricato al trattamento dei dati
4. Modulo per il rilascio del consenso dei dati personali
5. Documento 1 - Diagrammi di flusso della gestione dei processi operativi definiti:
    - Flusso Determina Direttore;
    - Flusso Determina Dirigente;
    - Flusso Determina Rup Direttore;
    - Flusso Determina Rup Dirigente.

6. Organigramma
7. RomaNatura_GDPR_DPIA - Determine
8. RomaNatura_GDPR_DPIA - Ammende
9. RomaNatura_GDPR_DPIA – Dipendenti
10. RomaNatura_GDPR_DPIA – Fornitori/ Clienti
11. RomaNatura_GDPR_DPIA – Nulla Osta
12. RomaNatura_GDPR_DPIA - Videsorveglianza (N/A)

Il presente documento costituito da 71 pagine è stato interamente letto ed approvato dalla Direzione,sottoscritto e datato nell'ultima pagina.

Data Firma

_____ _____