PUBBLICA CONSULTAZIONE

Codice di Condotta per gli Ordini Territoriali dei Medici Veterinari

Promosso dagli Ordini Territoriali dei Medici Veterinari delle provincie di: Agrigento, Brindisi, Catania, Chieti, Como e Lecco, Cremona, Isernia, L'Aquila, Mantova, Messina, Novara, Pescara, Pordenone, Potenza, Taranto, Trento, Treviso, Varese e Vicenza

CODICE DI CONDOTTA PER GLI ORDINI TERRITORIALI DEI MEDICI VETERINARI

PUBBLICA CONSULTAZIONE

INDICE DEI CONTENUTI

PREAMBOLO E PREMESSA

Il presente Codice di Condotta (di seguito anche Codice) è il frutto di una collaborazione tra gli Ordini Territoriali dei Medici Veterinari delle provincie di Agrigento, Brindisi, Catania, Chieti, Como e Lecco, Cremona, Isernia, L'Aquila, Mantova, Messina, Novara, Pescara, Pordenone, Potenza, Taranto, Trento, Treviso, Varese e Vicenza (di seguito Ordini Territoriali Promotori). Lo scopo della collaborazione è quello di realizzare, a beneficio degli Ordini Territoriali dei Medici Veterinari delle provincie italiane (di seguito anche Ordini Territoriali) uno strumento duttile ed intuitivo che possa essere di ausilio agli stessi per affrontare e gestire efficacemente gli adempimenti in materia di Privacy.

L'adozione di questo strumento può quindi contribuire a migliorare nei singoli Ordini Territoriali la conformità alla normativa di protezione dei Dati Personali, avendo come effetto sia la riduzione dei rischi di sanzione che possono derivare da non conformità e/o non "compliance" rispetto al GDPR, sia la promozione della cultura della Privacy e della tutela dei Dati Personali in generale.

L'Ordine Territoriale dei Medici Veterinari è un Ente privato di diritto pubblico, formato da tutti i Medici Veterinari Iscritti nell'Albo.
Esso assume notevole importanza ed autorità nell'ambito dell'esercizio della professione veterinaria. Si pensi ad esempio all'obbligo di iscrizione del medico veterinario all'Albo per poter esercitare la professione ed al potere disciplinare attribuito dalla legge ai Consigli Direttivi degli Ordini Territoriali dei Medici Veterinari.
Al Consiglio Direttivo dell'Ordine Territoriale, eletto tra tutti i Medici Veterinari iscritti nell'Albo, sono assegnati precisi compiti istituzionali ed amministrativi:

- la difesa del decoro e della indipendenza della professione a salvaguardia dell'utente, delle persone e degli animali;
- la promozione del progresso culturale e della conoscenza medica degli iscritti;
- la collaborazione con le autorità centrali e periferiche dando pareri e formulando proposte su aree di specifica competenza;
- la composizione di controversie fra iscritti e fra iscritto e cliente;
- l'esercizio del potere disciplinare.

I Medici Veterinari hanno inoltre una notevole rilevanza pubblica: oltre a prevenire e curare le malattie negli animali, tra le tante attività loro attribuite evidenziamo le seguenti funzioni:

- prevenire le zoonosi (malattie infettive trasmissibili dagli animali all'uomo);

- supportare gli allevamenti zootecnici nella qualificazione della propria produzione;
- elevare il livello biotecnologico aziendale;
- garantire i consumatori sulla qualità e sulla salubrità dei prodotti;
- educare allevatori e popolazione a una corretta igiene ambientale e sanitaria.

Per l'importanza dei compiti pubblici loro attribuiti gli Ordini Territoriali dei Medici Veterinari sono considerati Enti Pubblici di Diritto Pubblico e quindi – pur non ricevendo alcun sostegno economico dallo Stato ed essendo sostenuti solamente dai contributi dei propri iscritti – sono **assoggettati al rispetto di tutte le regole** che gravano sulle Pubbliche Amministrazioni.
La sproporzione tra risorse economiche, estremamente ridotte, e quantità ed onerosità dei compiti attribuiti, comporta che le attività richiedenti risorse umane siano spesso basate sul volontariato ***pro-bono*** dei componenti del Consiglio Direttivo dell'Ordine Territoriale.

I Dati Personali trattati dagli Ordini Territoriali dei Medici Veterinari non sono costituiti solamente da dati comuni. In relazione ai compiti istituzionali loro attribuiti, gli Ordini Territoriali dei Medici Veterinari gestiscono anche Dati Personali relativi a contenziosi o procedure giudiziarie, dati particolari relativi allo stato di salute ed alla vulnerabilità economica del Medico Veterinario.

Nonostante l'esiguità delle risorse a disposizione, gli Ordini Territoriali dei Medici Veterinari hanno l'obbligo/necessità di:

- **conseguire un adeguato livello di protezione** dei Dati Personali da trattati;
- **ricorrere a consulenti esperti** e qualificati sulle norme del GDPR**;**
- **rispettare la normativa** Privacy in vigore;
- **garantire elevate tutele di protezione** agli Interessati.

Questo Codice di Condotta vuole essere un sostanziale aiuto agli Ordini Territoriali dei Medici Veterinari Italiani per comprendere meglio e rispettare la normativa sulla Protezione dei Dati Personali.

All'interno di questo Codice di Condotta, ovviamente limitatamente ai trattamenti che le competono, la Federazione Nazionale viene considerata quale Titolare Autonomo del Trattamento: di questo dovrà essere tenuto conto nello sviluppo del Modello Organizzativo Privacy di ciascun Ordine Territoriale dei Medici Veterinari.

I contenuti di questo documento (linee guida, suggerimenti, esempi, allegati etc. etc.) sono il frutto di un lungo e attento lavoro di raccolta e analisi dello stato attuale dei Registri dei Trattamenti e della documentazione fornita dagli Ordini Territoriali dei Medici Veterinari che si sono resi disponibili a collaborare con il Gruppo di Lavoro.
Il risultato di questo lavoro costituisce un'architettura logica idonea a supportare

una completa revisione dei Modelli Organizzativi Privacy degli Ordini Territoriali dei Medici Veterinari.
I suggerimenti e le regole proposte potranno adottate in brevissimo tempo per elevare il livello di compliance alla normativa di protezione dei Dati Personali e conseguentemente elevare il livello di tutela dei Dati Personali degli Interessati.
La serie di regole, misure e prescrizioni suggerite, pur nella loro facilità di adozione, saranno determinanti per il raggiungimento della compliance; si pensi al miglioramento che potrebbe essere introdotto dalla nomina di un Responsabile Protezione Dati (RPD) "di gruppo", rispetto ad alcune nomine che potrebbero essere assegnate a soggetti privi delle indispensabili competenze, senza la necessaria indipendenza ed autonomia o, addirittura, in conflitto di interessi.

Il Gruppo di Lavoro, che ha collaborato alla progettazione, stesura e validazione di questo Codice di Condotta, ritiene anche fondamentale il contributo rappresentato dagli allegati al Codice (gli schemi operativi contestualizzati, le procedure di riferimento indicate, i documenti di esempio) in quanto costituiscono una importante base operativa e di conoscenza sulla quale impostare – o migliorare – le procedure sinora adottate dall'Ordine Territoriale.

L'adozione di questo Codice di Condotta può quindi costituire un punto di svolta significativo nel necessario processo di miglioramento continuo che deve essere *motore* di ogni sistema di gestione della Privacy.

In esso sono state rispettate le quattro fasi del cosiddetto "Ciclo di Deming" (o ciclo di PDCA, acronimo dall'inglese Plan–Do–Check–Act, in italiano "Pianificare - Fare - Verificare - Agire"), metodo di gestione iterativo in quattro fasi che viene utilizzato per il controllo e il miglioramento continuo dei processi e dei prodotti:

- è stato pianificato ed adottato un sistema di trattamento dei Dati Personali;
- è stato effettuata una serie di check di controllo;
- sono stati verificati i risultati delle verifiche;
- sono state identificate le corrispondenti misure di miglioramento.

ARTICOLO 1 - AMBITO DI APPLICAZIONE

Il presente Codice è riferito alle attività di trattamento dei Dati Personali relativi alle persone fisiche trattati dagli Ordini Territoriali dei Medici Veterinari limitatamente al territorio dello Stato italiano ed è applicabile unicamente a livello nazionale.

Non si applica ai Trattamenti effettuati al di fuori del territorio italiano. È quindi concepito come un Codice Nazionale, soggetto esclusivamente all'Autorità italiana per la Protezione dei Dati Personali e redatto solo in lingua italiana.
Ai sensi dell'art. 40 del Regolamento la sua approvazione è richiesta al Garante per la protezione dei Dati Personali, in qualità di Autorità di Controllo competente ai sensi dell'art. 55 del Regolamento.

ARTICOLO 2 - DEFINIZIONI E ALLEGATI

Sulla base delle considerazioni indicate nella Premessa, per facilitare e garantire una corretta ed immediata interpretazione delle norme sulla protezione dei Dati Personali, ovvero per rendere più agevole lo studio e l'interpretazione di questo Codice ed anche del GDPR, si riportano nel seguito alcune definizioni dei termini usati nell'ambito di questo Codice di Condotta.

Qualora nelle esemplificazioni riportate comparissero elenchi di Dati Personali, tali elenchi non devono essere considerati esaustivi ma andranno verificati con la specifica situazione del singolo Ordine Territoriale.

Definizioni

1. **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile. Ciò può includere nomi, indirizzi, numeri di telefono, indirizzi e-mail, dati di identificazione biometrici, dati sanitari e altre informazioni che consentono di identificare una persona specifica.
2. **Interessato**: la persona fisica identificata o identificabile a cui si riferiscono i Dati Personali. In un contesto veterinario, gli Interessati possono includere i pazienti animali, i proprietari degli animali e altre parti coinvolte nella pratica veterinaria.
3. **Trattamento dei Dati Personali**: Indica qualsiasi operazione o insieme di operazioni effettuate su Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, la consultazione, l'uso, la divulgazione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, l'eliminazione o la distruzione dei Dati Personali.

4. **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; nel nostro caso l'Ordine Territoriale dei Medici Veterinari.

5. **Responsabile del trattamento**: l'organizzazione o la persona fisica che tratta i Dati Personali per conto del Titolare del trattamento, agendo su istruzioni del Titolare stesso.
6. **Autorizzato/Incaricato del trattamento**: la persona fisica autorizzata a compiere operazioni legate all'utilizzo dei Dati Personali per conto del Titolare del trattamento (o del Responsabile del trattamento).
7. **Destinatario**: la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo a cui sono comunicati i Dati Personali, indipendentemente dal fatto che sia un terzo o meno.
8. **Responsabile della Protezione dei Dati (RPD o DPO):** la persona fisica incaricata di sovrintendere alla corretta applicazione delle norme sulla Privacy e di garantire il rispetto del GDPR all'interno dell'Ordine Territoriale dei Veterinari; il Responsabile della Protezione che può essere sia interno che esterno all'organizzazione.
9. **Informativa**: è il documento o la comunicazione fornita all'interessato per informarlo in modo trasparente, chiaro e conciso sul trattamento dei suoi Dati Personali da parte dell'Ordine dei Veterinari. L'informativa è uno degli elemento fondamentali per garantire la conformità al GDPR e per tutelare i diritti degli Interessati.
10. **Diritti degli Interessati**: sono i diritti, riconosciuti come fondamentali, che gli Interessati hanno in relazione al trattamento dei loro Dati Personali. I principali diritti sono il diritto di accesso, quello di rettifica, di cancellazione, di limitazione del trattamento, di portabilità dei dati, di opposizione al trattamento ed infine quello di revoca del consenso precedentemente dato.
11. **Consenso**: Si riferisce all'espressione di volontà, libera, specifica, informata e inequivocabile dell'interessato mediante la quale quest'ultimo accetta il trattamento dei suoi Dati Personali per uno o più scopi specifici.
12. **DPIA (Data Protection Impact Assessment):** valutazione dell'impatto sulla protezione dei Dati Personali, che consiste in una valutazione sistematica di fattori relativi al trattamento dei Dati Personali, finalizzata a valutare i rischi per i diritti e le libertà delle persone fisiche derivanti da tale trattamento.
13. **Violazione dei Dati Personali (Data Breach):** indica una violazione della sicurezza che provoca, accidentalmente o in modo illecito, la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso non autorizzato ai Dati Personali trasmessi, conservati o comunque trattati.

14. **Elaborazione su larga scala:** trattamento di Dati Personali che coinvolge una grande quantità di Interessati, un vasto territorio geografico o riguardante Dati Personali sensibili o giudiziari.
15. **Privacy by Design:** l'approccio secondo il quale la protezione dei Dati Personali deve essere integrata fin dall'inizio nello sviluppo di sistemi, prodotti e servizi, adottando misure tecniche e organizzative adeguate per garantire il rispetto della Privacy.
16. **Privacy by Default:** l'adozione di misure tecniche e organizzative adeguate per garantire che, per impostazione predefinita, siano trattati solo i Dati Personali necessari per le specifiche finalità del trattamento e che questi dati non siano accessibili a un numero indeterminato di persone senza intervento esplicito dell'interessato.
17. **Reclamo:** è una istanza mediante la quale un individuo o una organizzazione si rivolge all'Autorità di Controllo competente per segnalare una presunta violazione delle norme sulla protezione dei Dati Personali.
18. **Autorità di Controllo**: L'organismo indipendente Responsabile della Protezione dei Dati Personali nell'ambito del territorio nazionale, Responsabile del monitoraggio dell'applicazione delle norme sulla protezione dei dati, della adozione di decisioni in merito al trattamento dei Dati Personali, dell'emanazione di sanzioni in caso di violazioni. Nel contesto italiano, il Garante Privacy è l'Autorità Garante per la Protezione dei Dati Personali.

Al presente Codice di Condotta, con lo scopo di facilitare agli Ordini Territoriali la messa a regime del proprio Organigramma Privacy, sono allegati i seguenti documenti:

1. **Esempio di Informativa del Sito Web;**
2. **Esempio di nomina di Soggetto Autorizzato;**
3. **Esempio di nomina di Responsabile Esterno;**
4. **Esempio di Registro dei Trattamenti;**
5. **Esempio di Registro dei Data Breach.**

ARTICOLO 3 - L'INFORMATIVA AGLI INTERESSATI

Nel contesto del Codice di Condotta ai sensi del GDPR per gli Ordini Territoriali dei Medici Veterinari, l'informativa rappresenta un elemento fondamentale per garantire la conformità al GDPR e per tutelare i diritti degli Interessati, informandoli in modo trasparente, chiaro e conciso sul trattamento dei loro Dati Personali da parte dell'Ordine Territoriale dei Medici Veterinari.

L'informativa che l'Ordine Territoriale dei Medici Veterinari deve predisporre conterrà le seguenti informazioni:

- **Identità del Titolare del trattamento:** deve essere chiaramente indicato l'Ordine Territoriale dei Medici Veterinari.
- **Finalità del trattamento:** devono essere indicate le ragioni per le quali i Dati Personali degli Interessati vengono trattati (ad es. adempimento di obblighi professionali, gestione degli iscritti, tutela della salute pubblica, ecc.).
- **Tipologia dei Dati Personali trattati:** occorre specificare quali tipi di Dati Personali vengono raccolti e trattati dall'Ordine Territoriale (ad es. nome, indirizzo, numero di telefono, indirizzo e-mail, informazioni professionali, ecc.).
- **Base giuridica del trattamento:** va indicata su quale base legale si fonda il trattamento che viene effettuato sui Dati Personali (ad esempio: **Consenso**, Adempimenti di **Obblighi Contrattuali**, **Obblighi di Legge** cui è soggetto il Titolare, **Salvaguardia degli Interessi Vitali di un Terzo**, **Interesse Pubblico** o Esercizio di Pubblici Poteri da parte del Titolare, **Legittimo Interesse** Prevalente di un Titolare o di un Terzo).
- **Destinatari dei Dati Personali**: gli Interessati devono essere informati su eventuali terze parti o categorie di destinatari a cui i Dati Personali potrebbero essere comunicati (ad esempio autorità competenti, istituzioni sanitarie, ecc.).
- **Trasferimento internazionale dei dati:** Se i Dati Personali vengono trasferiti al di fuori dell'Unione Europea, è necessario indicare i paesi destinatari e le misure di sicurezza adottate per garantire la protezione dei dati durante il trasferimento.
- **Periodo di conservazione dei dati:** Bisogna specificare il periodo per cui verranno conservati i Dati Personali o i criteri utilizzati per determinare tale periodo.
- **Diritti degli Interessati:** L'informativa dovrebbe informare gli Interessati sui loro diritti in merito ai loro Dati Personali, come il diritto di accesso, il diritto di rettifica, il diritto alla cancellazione, il diritto di opposizione, il diritto alla portabilità dei dati, ecc.
- **Modalità di esercizio dei diritti:** Bisogna indicare come gli Interessati possono esercitare i loro diritti, ad esempio fornendo un indirizzo e-mail o un modulo specifico.
- **Reclami:** È importante informare gli Interessati sulla possibilità di presentare un reclamo all'Autorità di Controllo competente, se ritengono che il trattamento dei loro Dati Personali violi il GDPR.

Nella redazione dell'informativa è essenziale usare un linguaggio chiaro e comprensibile a chiunque, evitando l'uso di termini tecnici complessi.

ARTICOLO 4 - RESPONSABILITÀ DELL'ORDINE TERRITORIALE DEI MEDICI VETERINARI

1. L'Ordine Territoriale dei Medici Veterinari riconosce che la assegnazione di ruoli e responsabilità e la costante promozione all'interno dell'Ordine Territoriale della cultura della Protezione dei Dati Personali costituiscono gli strumenti più efficaci per garantire il rispetto delle norme del Regolamento Generale sulla Protezione dei Dati (GDPR).
2. L'Ordine Territoriale dei Medici Veterinari svolge il ruolo di Titolare del trattamento per i Dati Personali raccolti e trattati nel contesto delle sue attività istituzionali, amministrative e regolamentari: in questa veste l'Ordine Territoriale dei Medici Veterinari determina le finalità ed i mezzi di trattamento dei Dati Personali degli iscritti in tutte le attività svolte in relazione alla gestione e all'amministrazione degli iscritti.
3. Con riferimento alla Protezione dei Dati Personali (GDPR) ed alla adozioneo del presente Codice di Condotta all'interno dell'Ordine Territoriale dei Medici Veterinari, i ruoli e le responsabilità relative vengono definite come segue:
    a. **Consiglio dell'Ordine Territoriale:** è Responsabile dell'approvazione, dell'implementazione e della revisione delle politiche, delle procedure e delle misure di sicurezza in conformità al GDPR. Ha l'obbligo di promuovere la cultura della protezione dei dati e di fornire le risorse necessarie per garantire la conformità.
    b. **Responsabile della Protezione dei Dati (RPD):** è Responsabile della supervisione e del monitoraggio della conformità al GDPR all'interno dell'Ordine Territoriale dei Medici Veterinari. Fornisce consulenza, supporto e supervisione nella gestione e nella protezione dei Dati Personali. Collabora con l'Autorità di Controllo competente e agisce come punto di contatto per le richieste e le comunicazioni relative alla protezione dei dati.
    c. **Dipendenti e collaboratori:** i dipendenti e i collaboratori dell'Ordine Territoriale dei Medici Veterinari sono responsabili di aderire alle politiche, alle procedure e alle misure di sicurezza stabilite per proteggere i Dati Personali degli iscritti. Devono essere istruiti, devono ricevere formazione regolare sulla protezione dei dati e agire in conformità alle disposizioni del GDPR.
    d. **Iscritti:** gli iscritti all'Ordine Territoriale dei Medici Veterinari sono tenuti a rispettare le disposizioni del GDPR e a fornire informazioni accurate e complete in merito ai propri Dati Personali all'Ordine Territoriale. Devono essere consapevoli dei loro diritti in materia di protezione dei dati e collaborare con l'Ordine Territoriale per garantire il trattamento corretto e sicuro delle loro informazioni personali.

4. L'Ordine Territoriale dei Medici Veterinari si impegna a promuove la comunicazione e la consapevolezza riguardo ai ruoli e alle responsabilità relative alla protezione dei Dati Personali. Ciò avverrà sia attraverso la divulgazione del presente Codice di Condotta GDPR, sia mediante sessioni di formazione periodiche ed anche ricorrendo alla pubblicazione di linee guida sulla protezione dei dati.
5. L'Ordine Territoriale dei Medici Veterinari si impegna a istituire un processo di revisione periodica dei ruoli e delle responsabilità, al fine di assicurare che gli stessi siano aggiornati e adeguati all'evoluzione normativa e alle esigenze dell'Ordine Territoriale.
6. L'Ordine Territoriale dei Medici Veterinari si impegna a fornire agli iscritti le linee guida e le informazioni necessarie per comprendere e adempiere ai propri ruoli e responsabilità in materia di protezione dei Dati Personali, incluso il rispetto delle disposizioni del GDPR e delle leggi nazionali applicabili sulla protezione dei dati.
7. È responsabilità dell'Ordine Territoriale dei Medici Veterinari garantire che gli iscritti siano adeguatamente informati sui principi fondamentali del trattamento dei Dati Personali, inclusi i principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, accuratezza, limitazione della conservazione, integrità e riservatezza.
8. L'Ordine Territoriale dei Medici Veterinari ricorda ai propri iscritti che sono tenuti a trattare i Dati Personali in conformità con le disposizioni del GDPR, a rispettare la riservatezza dei dati, ad adottare le adeguate misure di sicurezza per proteggere i Dati Personali da accessi non autorizzati, perdita o divulgazione, a rispettare i diritti degli Interessati, come definiti dal GDPR, inclusi i diritti di accesso, rettifica, cancellazione e opposizione.
9. L'attuale struttura del Codice Deontologico dei Medici Veterinari consente all'Ordine Territoriale di adottare misure disciplinari o sanzioni nei confronti degli iscritti che violino le disposizioni del GDPR o del presente Codice di Condotta, nel rispetto delle norme e dei principi di equità e proporzionalità.
10. Nel caso di violazione dei Dati Personali (Data Breach), l'Ordine Territoriale dei Medici dei Veterinari si impegna a notificare tempestivamente l'incidente all'Autorità di Controllo competente (comunque entro le 72 ore) e, nel caso in cui ricorrano i presupposti di cui all'art. 34 del Regolamento, comunicarlo anche agli iscritti Interessati, fornendo informazioni complete sulle circostanze dell'incidente, sulle possibili conseguenze e sulle misure adottate per affrontare la situazione.
11. L'Ordine Territoriale dei Medici dei Veterinari si impegna a collaborare attivamente con le Autorità di Controllo competenti nel caso di indagini o verifiche sulla conformità al GDPR e ad adottare le misure correttive necessarie nel

caso in cui si riscontrino violazioni delle norme sulla protezione dei Dati Personali.

12. L'Ordine Territoriale dei Medici dei Veterinari si impegna a mantenere un registro delle attività di trattamento dei Dati Personali svolte, in conformità alle disposizioni del GDPR, e a renderlo disponibile all'Autorità di Controllo competente su richiesta.

ARTICOLO 5 - FINALITÀ DEL CODICE DEGLI ORDINI TERRITORIALI

I 19 Ordini Territoriali Promotori intendono accogliere l'invito contenuto nel "considerando 98" del Regolamento UE 2016/679.

Il presente Codice di Condotta, elaborato sulla base degli art. 40 e 41 del Regolamento, persegue la finalità di facilitare gli Ordini Territoriali dei Medici Veterinari nell'effettiva applicazione del Regolamento relativamente ai Trattamenti dei Dati Personali delle persone fisiche, tenendo conto delle caratteristiche specifiche dei Trattamenti effettuati, delle esigenze specifiche degli Ordini Territoriali stessi, del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche, della sicurezza dei dati e del rispetto dei diritti degli Interessati.

Una ulteriore finalità è costituita dal rafforzamento della fiducia pubblica rispetto alla funzione svolta dagli Ordini Territoriali dei Medici Veterinari (e di conseguenza anche rispetto alla professione veterinaria), assicurando trasparenza, integrità e professionalità in tutte le attività svolte dagli Ordini Territoriali.

ARTICOLO 6 - DATI PERSONALI TRATTATI DAGLI ORDINI TERRITORIALI

Gli Ordini Territoriali dei Medici Veterinari possono trattare una serie di Dati Personali, che possono variare a seconda del contesto e delle finalità del trattamento.

Di seguito sono elencati, a titolo non esaustivo, alcuni esempi comuni di Dati Personali che potrebbero essere trattati:

1. **Informazioni di identificazione personale**: includono nome, cognome, data di nascita, luogo di nascita, genere, nazionalità, numero di identificazione personale, come il codice fiscale o il numero di carta d'identità.
2. **Informazioni di contatto**: includono indirizzo di residenza, indirizzo e-mail, numero di telefono e fax.
3. **Dati professionali**: informazioni relative alla pratica professionale, come la qualifica, l'iscrizione all'Ordine Territoriale, l'eventuale specializzazione, l'esperienza professionale.
4. **Storia lavorativa**: informazioni riguardanti l'esperienza lavorativa del medico

veterinario, come gli impieghi precedenti, le date di assunzione e di cessazione del rapporto di lavoro, le posizioni ricoperte e le responsabilità professionali.

5. **Dati di formazione ed educazione**: informazioni riguardanti la formazione accademica, i corsi di specializzazione seguiti, i titoli di studio conseguiti e le certificazioni professionali.
6. **Dati finanziari**: informazioni finanziarie, come coordinate bancarie o modalità di pagamento.
7. **Dati disciplinari**: informazioni riguardanti eventuali procedimenti disciplinari o indagini in corso nei confronti del medico veterinario, comprese le sanzioni disciplinari adottate o le eventuali restrizioni professionali.
8. **Dati di comunicazione**: registrazioni di comunicazioni, ad esempio e-mail o documenti inviati o ricevuti.

Tali categorie di Dati Personali possono essere sottoposte a tecniche di anonimizzazione o pseudoanonimizzazione nei casi e con le modalità di seguito descritte.
Le tecniche di anonimizzazione rendono le informazioni che si riferiscono a una persona fisica identificata o identificabile tali da impedire o da non consentire più l'identificazione dell'Interessato.
Le tecniche di pseudoanonimizzazione riducono il rischio di identificazione diretta degli Interessati in quanto i Dati Personali non possono più essere attribuiti a un Interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile.
È vietata l'acquisizione, la duplicazione e/o l'archiviazione di Dati Personali degli Interessati presenti nella documentazione sanitaria, per mezzo di dispositivi personali o con modalità difformi da quelle previste dal presente Codice.
La violazione di tali misure è fonte di responsabilità, anche disciplinare.

ARTICOLO 7 - INFORMAZIONI DA RENDERE ALL'INTERESSATO ED EVENTUALE CONSENSO

Gli Ordini Territoriali dei Medici Veterinari, ed i Medici Veterinari che svolgono la professione, hanno diversi destinatari delle proprie Informative per il trattamento dei Dati Personali. Tali soggetti possono essere:

- gli Iscritti,
- i Proprietari degli Animali,
- i Consulenti e Fornitori,
- gli Enti pubblici a cui comunicano i dati.

Il primo obbligo a carico del Professionista veterinario, indipendentemente dalle dimensioni del proprio studio professionale, è quello di informare il proprietario

dell'animale circa la natura dei dati raccolti e le finalità in ragione delle quali sono raccolti, e circa le modalità di trattamento e conservazione dei dati stessi.
I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, par. 1, e 14, par. 1, del Regolamento.
In particolare, l'informativa deve sempre specificare:

- i dati di contatto del Titolare e del suo rappresentante (se esistente);
- i dati di contatto del Responsabile della Protezione dei Dati (RPD o DPO secondo l'acronimo inglese di Data Protection Officer) ove esistente;
- le finalità e le basi giuridiche dei diversi Trattamenti;
- l'eventuale legittimo interesse, se quest'ultimo costituisce la base giuridica del trattamento e la documentazione dei motivi sui quali si fonda;
- eventuali destinatari o categorie di destinatari;
- se si trasferiscono i Dati Personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: se si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; se si utilizzano norme vincolanti d'impresa, in inglese Binding Corporate Rules - BCR; se sono state inserite specifiche clausole contrattuali standard, ecc.).

Il Regolamento prevede anche ulteriori informazioni in quanto necessarie per garantire un trattamento corretto e trasparente. In particolare, il Titolare deve specificare:

- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo;
- la possibilità di revocare in qualsiasi momento il consenso al trattamento;
- l'esistenza del diritto, per l'interessato, di chiedere l'accesso ai Dati Personali che lo riguardano, la rettifica, la cancellazione, la limitazione del trattamento o il diritto di opporsi allo stesso, nonché il diritto alla portabilità dei dati;
- il diritto di presentare un reclamo a un'Autorità di Controllo, che in Italia è il Garante per la protezione dei Dati Personali.

ARTICOLO 8 - MISURE DI ACCOUNTABILITY

Il concetto di **accountability**, introdotto dal GDPR, costituisce una delle più rilevanti innovazioni del Regolamento, ed un cambio di passo fondamentale nella normativa di protezione dei Dati Personali.
Con l'accountability (responsabilizzazione) si è passati da una normativa di tipo prescrittivo ad un modello organizzativo *proattivo*, nel quale le fondamenta sono la gestione del rischio, la responsabilità e la documentazione della conformità.
Da questo la necessità – per Titolari e Responsabili del trattamento - di acquisire un nuova visione della tutela dei Dati Personali, maturare una maggiore consapevolezza, definire nuove strategie di protezione, non meramente reattive ma preventive.

Inoltre diviene necessario dotarsi di misure adeguate, personalizzate sulle peculiarità della organizzazione, peculiarità che non sono statiche ma si adeguano di continuo ai cambiamenti delle tipologie, dei processi, degli strumenti di trattamento, mantenendo sempre l'attenzione rivolta alla valutazione del rischio.
Il concetto di **accountability** previsto nel Regolamento è un approccio orientato alla responsabilità.
Le organizzazioni devono essere in grado di dimostrare di:

- aver raggiunto un **adeguato livello di consapevolezza** rispetto alla normativa sulla protezione dei Dati Personali;
- aver adottato **misure adeguate** a mantenere i Dati Personali in sicurezza;
- poter **rendicontare** e **giustificare** le loro scelte ed azioni, in caso di ispezioni o di richieste della Autorità di Controllo nazionale.

Questo approccio viene richiesto per garantire una maggiore trasparenza e fiducia nella gestione dei Dati Personali nei confronti di tutti i titolari del trattamento, da parte delle persone che conferiscono i loro Dati Personali.
Quindi **accountability** anche come assicurazione – nei confronti degli Interessati - di maggiore trasparenza e fiducia nel trattamento dei loro Dati Personali, e non solo per adeguarsi alle esigenze normative; accountability alla base del *rapporto fiduciario* con coloro che affidano i loro Dati Personali ai titolari del trattamento.
Nel panorama europeo, in cui la tutela della Privacy rappresenta, oltre che un diritto consolidato dei cittadini, una base della economia digitale presente e futura, l'accountability dei titolari emerge come il **fondamento** su cui costruire una solida cultura di rispetto e tutela dei Dati Personali.
Le misure di accountability previste da questo Codice di Condotta sono:

- **La nomina dell'RPD**
  Tra le innovazioni introdotte dal Regolamento, la più significativa è la figura del Responsabile della Protezione dei Dati Personali; si tratta certamente di una risposta alla crescente complessità delle sfide portate dalla protezione dei Dati Personali nel contesto moderno; il RPD, con la sua azione indipendente, competente e promotrice, funge da baluardo contro potenziali violazione della Privacy, garantendo altresì una maggiore conformità della organizzazione. Proprio per questo il Regolamento ha reso tale nomina obbligatoria non solo in ogni organizzazione pubblica, ma anche in quelle private che trattano, su larga scala, Dati Personali meritevoli di una protezione rafforzata. In questi anni, le varie organizzazioni che hanno nominato un RPD (eventualmente anche un RPD di gruppo nei casi di realtà ridotte o meno complesse) hanno beneficiato di un sensibile miglioramento della loro *cultura Privacy*, elevando contestualmente la conformità normativa e, come riflesso primario, la protezione dei Dati Personali loro affidati.

- **La definizione dei ruoli dei soggetti implicati nei Trattamenti**
  La definizione di ruoli chiari e ben definiti per i soggetti coinvolti nel trattamento dei Dati Personali aiuta a definire le responsabilità e le competenze di ciascuna figura all'interno dell'organizzazione. Questo assicura che ogni persona coinvolta nel trattamento dei dati sia a conoscenza delle proprie responsabilità e sappia come agire in conformità con la normativa di protezione.
- **La tenuta di un organigramma Privacy**
  L'organigramma Privacy rappresenta la struttura organizzativa relativa alle attività di trattamento dei Dati Personali all'interno dell'organizzazione. Questo organigramma deve indicare chiaramente le varie figure coinvolte nel trattamento dei dati, i loro ruoli e le interconnessioni tra di loro. L'organigramma Privacy fornisce una visione chiara dell'organizzazione in relazione alle attività di trattamento dei dati, aiutando l'Autorità di Controllo a comprendere come l'organizzazione si stia attivando per garantire la protezione dei Dati Personali e il rispetto del GDPR.
- **La valutazione dei rischi che gravano sui Trattamenti**
  La valutazione del rischio che incombe su ogni trattamento è una delle misure più importanti che un Titolare o Responsabile del trattamento possa mettere in atto per proteggere al meglio i Dati Personali affidatigli, in quanto tale attività consente di porre in atto procedure ed impostazioni degli strumenti tesi a minimizzare il rischio.
- **L'elaborazione di una DPIA in caso di Trattamenti soggetti artt. 35 o 36**
  Le DPIA sono valutazioni approfondite dei rischi connessi a specifiche attività di trattamento dei dati che potrebbero comportare un rischio elevato per i diritti e le libertà degli Interessati. Le organizzazioni, qualora ne ricorrano gli estremi, devono condurre una DPIA preliminare per identificare e affrontare i rischi in modo proattivo.
- **La relazione annuale dell'RPD**
  Al termine dell'anno il Responsabile della Protezione dei Dati relaziona sulle attività svolte, sulle richieste pervenute dagli Interessati, ed in generale sui fatti avvenuti aventi rilievo in tema data protection.

- **La redazione e l'aggiornamento del Registro dei Trattamenti**
  In generale, le Organizzazioni che effettuino Trattamenti che possano presentare un livello di rischio - anche non particolarmente elevato – per i diritti e le libertà degli Interessati, devono mantenere un registro di tutte le

attività di trattamento dei Dati Personali; questo strumento rappresenta un elevato livello di conformità con la normativa di protezione da parte della organizzazione, serve a rispondere ad eventuali ispezioni o richieste dell'Autorità di Controllo, ma soprattutto getta le basi per ulteriori attività fondamentali, quali la valutazione e l'analisi del rischio che incombe sui Trattamenti. All'adozione del registro dei Trattamenti, costituendo questa una misura essenziale, è dedicato un apposito articolo di questo CdC (vedasi al prossimo art. 12).

- **Privacy by Design e Privacy by Default**
  I Titolari del trattamento devono prevedere la protezione dei dati fin dall'inizio nello sviluppo dei prodotti, dei servizi e dei processi. Ciò significa prendere in considerazione la protezione dei dati fin dalla fase di progettazione (Privacy by Design) e assicurarsi che, per impostazione predefinita, siano raccolti solo i dati necessari per uno specifico scopo di trattamento (Privacy by Default).
- **Garanzie sui trasferimenti internazionali di dati**
  Nel caso che i Dati Personali debbano essere trasferiti al di fuori dell'Unione europea, i titolari del trattamento devono ottenere garanzie dai riceventi extra-UE, affinché siano adottate misure adeguate a proteggere tali dati, ottenendo un livello paragonabile a quello concesso dal Regolamento UE. Ciò potrebbe includere l'utilizzo di clausole contrattuali standard, norme vincolanti, la certificazione nel caso di società aderenti a programmi di certificazione riconosciuti o l'adesione a regimi di certificazione o codici di condotta approvati.
- **La definizione dell'appropriato framework di sicurezza ITC**
  I titolari del trattamento devono adottare misure tecniche, logistiche ed organizzative adeguate a proteggere i Dati Personali da accessi non autorizzati, perdita della integrità, indisponibilità o distruzione imprevista. Questo può includere l'implementazione di procedure di sicurezza, l'uso di crittografia, la pseudoanonimizzazione dei dati.
- **La formazione del personale delegato ai Trattamenti**
  Il personale coinvolto nel trattamento dei Dati Personali dovrebbe ricevere una formazione adeguata sulla protezione dei dati e sulle normative del GDPR. La formazione aiuta a sensibilizzare il personale sugli aspetti chiave della protezione dei dati e sulla responsabilità nel trattamento dei Dati Personali.
- **Meccanismi di ricezione del consenso**
  Le organizzazioni dovrebbero implementare meccanismi semplici e trasparenti per ottenere il consenso degli Interessati al trattamento dei loro Dati Personali. Il consenso deve essere informato, specifico, libero e revocabile

in qualsiasi momento ed i meccanismi dovrebbero prevederlo in modo possibilmente automatizzato.

- **Contratti con i responsabili del trattamento**
  Quando gli Ordini Territoriali si rivolgono a terzi, incaricandoli di trattare Dati Personali per conto loro, debbono nominarli Responsabili del Trattamento, specificando in modo chiaro i Trattamenti attribuiti, le modalità con cui effettuarli, le responsabilità loro attribuite, le misure di sicurezza da adottare. Questa nomina a Responsabile Esterno può essere incorporata nel contratto stipulato, oppure costituire un documento a se stante.
- **La verifica e l'aggiornamento delle misure di sicurezza fisiche, logiche ed organizzative**
  Periodicamente occorre rivalutare l'efficacia delle misure di sicurezza già in essere, e se del caso adottarne di migliori o più adeguate a proteggere al meglio i Dati Personali trattati.
- **Definizione dei tempi di conservazione dei dati**
  Dovrebbero essere specificate le disposizioni relative alla conservazione dei Dati Personali, indicando i tempi di conservazione previsti e le procedure per l'eliminazione sicura dei dati al termine del periodo di conservazione.
- **Valutazione periodica della conformità**
  Gli Ordini Territoriali dovrebbero effettuare regolarmente, e almeno annualmente, i controlli della conformità delle attività di trattamento e l'audit delle misure di protezione dei dati, per valutare che siano adeguate e in linea con il GDPR; se del caso, adottarne ulteriori o con caratteristiche migliori o più adeguate a proteggere al meglio i Dati Personali trattati; le valutazioni periodiche aiutano a rappresentare a terzi un livello adeguato di responsabilizzazione.
- **Politiche e procedure interne**
  Gli Ordini Territoriali dovrebbero sviluppare e implementare politiche e procedure interne chiare e facilmente accessibili riguardanti il trattamento dei Dati Personali. Queste politiche dovrebbero definire le responsabilità del personale coinvolto nel trattamento dei dati e le misure di sicurezza da seguire.

- **Gestione delle richieste degli Interessati**
  Il Regolamento, agli artt. 15 e successivi, concede agli Interessati una serie di diritti che includono, tra gli altri, il diritto di accesso, di rettifica, di can-

cellazione, ed altri; una corretta gestione delle richieste dimostra la trasparenza e la correttezza dell'Ordine Territoriale nei confronti degli Interessati, sempre all'interno delle tempistiche previste dal Regolamento; anche gli eventuali reclami pervenuti dagli Interessati debbono essere gestiti con trasparenza, fornendo un canale attraverso il quale gli individui possono esprimere eventuali loro preoccupazioni ed ottenere risposte esaurienti a questioni relative al trattamento dei Dati Personali.

- **Gestione delle eventuali violazioni dei dati**
  Occorre predisporre procedure per gestire e notificare tempestivamente le violazioni dei Dati Personali all'Autorità di Controllo e, nei casi previsti, agli Interessati. Questa procedura di gestione delle violazioni deve essere ben documentata e registrata.

ARTICOLO 9 - NOMINA DEL RPD

Designazione del Responsabile della Protezione dei Dati personali (RPD)

L'Ordine Territoriale dei Medici Veterinari, in conformità con l'articolo 37 del Regolamento Generale sulla Protezione dei Dati (GDPR), è tenuto alla designazione di un Responsabile della Protezione dei Dati (RPD) per sovrintendere alla gestione e alla conformità del trattamento dei dati personali all'interno dell'Ordine.
Mentre per la scelta della figura del Commercialista, del Consulente del Lavoro, dell'Avvocato etc. l'Ordine Territoriale è agevolato dalla presenza di un Albo che ne garantisce un livello "base" di professionalità, la normativa attuale non prevede l'istituzione di un Albo dei "Responsabili della protezione dei dati" che possa attestare i requisiti e le caratteristiche di conoscenza, abilità e competenza di chi vi è iscritto. Il Garante ha inoltre chiarito che, per i candidati al ruolo di RPD, non c'è l'obbligo di possedere attestati formali delle competenze professionali.
D'altra parte tali attestati, (come le certificazioni delle competenze) rilasciati anche all'esito di verifiche al termine di un ciclo di formazione, possono rappresentare un utile strumento per consentire agli Ordini Territoriali una valutazione oggettiva sul possesso da parte del candidato di un livello adeguato di conoscenza della disciplina anche se non equivalgono a una "abilitazione" allo svolgimento del ruolo del RPD. Importantissimo è dunque valutare, tra le varie certificazioni, l'ente che l'ha rilasciata e la durata in ore della formazione che è stata erogata.

Caratteristiche del RPD

Le caratteristiche che un RPD deve possedere non sono solamente di carattere tec-

nico-professionale-giuridico-informatico. La sua conoscenza specialistica della legislazione e delle pratiche sulla protezione dei dati deve essere accompagnata dal possesso di particolari caratteristiche umane e qualità personali, che sono fondamentali perché l'RPD possa svolgere efficacemente il suo ruolo all'interno di un'organizzazione. Queste caratteristiche contribuiscono alla sua capacità di gestire questioni delicate relative alla Privacy e alla protezione dei dati, di comunicare efficacemente con diverse parti interessate e di promuovere una cultura della protezione dei dati all'interno dell'organizzazione.
Il Responsabile Protezione Dati (RPD) di un Ordine Territoriale dovrebbe possedere le seguenti caratteristiche umane: integrità e etica professionale, capacità di comunicazione e di risoluzione dei problemi, discrezione e riservatezza, capacità di lavorare in modo indipendente ed in team.

Queste qualità non solo aiutano il RPD a svolgere i suoi compiti specifici legati alla conformità e alla protezione dei dati, ma contribuiscono anche a stabilire una cultura della protezione dei dati all'interno dell'organizzazione, promuovendo la fiducia tra i dipendenti, i clienti e le parti interessate.

Il Responsabile della Protezione dei Dati (RPD) sarà una figura indipendente e imparziale: un professionista esperto e qualificato in materia di protezione dei dati personali, con conoscenze specialistiche del GDPR e delle leggi nazionali applicabili sulla protezione dei dati personali, nonché delle caratteristiche peculiari di un Ordine Territoriale.

Nella scelta del RPD l'Ordine Territoriale dei Medici Veterinari porrà particolare attenzione alla presenza di eventuali posizioni di "**conflitto di interesse**" ed al **requisito di indipendenza ed autonomia** che il RPD deve avere.

L'Ordine Territoriale dei Medici Veterinari garantirà quindi al RPD:

1. di poter agire in modo indipendente;
2. di non essere soggetto a conflitti di interesse nella sua funzione di supervisione del trattamento dei dati;
3. di non ricevere istruzioni sul modo di svolgere le sue attività di monitoraggio e consulenza;
4. di avere le risorse necessarie per svolgere le sue funzioni in modo efficace (includendo tra queste risorse finanziarie, risorse umane e accesso alle informazioni rilevanti per il trattamento dei dati personali);
5. di avere ruolo e responsabilità (rispetto alla protezione dei dati personali) chiaramente definiti e comunicati all'interno dell'Ordine Territoriale e noti a tutti i membri dell'Organizzazione.

Compiti del RPD

Il Responsabile della Protezione dei Dati (RPD) svolge le seguenti funzioni:

1. Monitora l'applicazione del GDPR e delle leggi nazionali applicabili in materia di protezione dei dati personali all'interno dell'Ordine Territoriale dei Medici Veterinari
2. Fornisce consulenza e supporto all'Ordine Territoriale dei Medici Veterinari, ai suoi dipendenti e ai suoi collaboratori in merito alle questioni relative alla protezione dei dati personali.
3. Collabora con l'Autorità di Controllo competente e agisce come punto di contatto per le richieste e le comunicazioni dell'Autorità di Controllo.
4. Sovrintende alla valutazione dei rischi e all'implementazione di adeguate misure di sicurezza per proteggere i dati personali degli iscritti.
5. Monitora e verifica l'efficacia delle politiche, delle procedure e delle misure di sicurezza adottate dall'Ordine Territoriale dei Medici Veterinari in relazione alla protezione dei dati personali.
6. Fornisce informazioni e istruzioni in merito ai diritti degli iscritti in materia di protezione dei dati personali, inclusi i diritti di accesso, rettifica, cancellazione e opposizione.
7. Collabora con l'Ordine Territoriale dei Medici Veterinari per garantire la formazione continua dei dipendenti e dei collaboratori sull'importanza della protezione dei dati personali e sulla conformità al GDPR.

Il Responsabile della Protezione dei Dati (RPD) collabora attivamente con l'Ordine Territoriale dei Medici Veterinari per garantire che tutte le politiche, le procedure e le pratiche interne siano conformi alle disposizioni del GDPR e che siano adottate le misure tecniche e organizzative adeguate per proteggere i dati personali degli iscritti.

Il Responsabile della Protezione dei Dati (RPD) svolge un ruolo di consulenza all'interno dell'Ordine Territoriale dei Medici Veterinari, fornendo orientamenti e consigli sul trattamento dei dati personali, sulla valutazione di impatto, sulla protezione dei dati (DPIA), sulla notifica delle violazioni dei dati e su altre questioni rilevanti per la protezione dei dati personali.
Il Responsabile della Protezione dei Dati (RPD) mantiene un registro delle attività di trattamento dei dati personali svolte dall'Ordine, comprese le finalità del trattamento, le categorie di dati personali trattati, i destinatari dei dati e le eventuali trasferimenti internazionali di dati.

Compiti dell'Ordine Territoriale

L'Ordine Territoriale dei Medici Veterinari comunica in modo chiaro e trasparente l'identità e i dati di contatto del Responsabile della Protezione dei Dati (RPD) agli iscritti, alle autorità di controllo competenti e al pubblico in generale.
Nel caso in cui il Responsabile della Protezione dei Dati (RPD) sia impossibilitato a svolgere le proprie funzioni, L'Ordine Territoriale dei Medici Veterinari provvede a

designare un sostituto adeguatamente qualificato e competente per garantire la continuità e la conformità delle attività di protezione dei dati personali.
Nel caso in cui L'Ordine Territoriale dei Medici Veterinari decida di cambiare il Responsabile della Protezione dei Dati (RPD), è tenuto a comunicare tale cambiamento all'Autorità di Controllo competente e a informare gli iscritti della nuova designazione.
L'Ordine Territoriale dei Medici Veterinari deve promuovere la cooperazione tra il RPD, l'organizzazione e l'Autorità di Controllo competente per la protezione dei dati.
Il RPD dovrebbe essere il punto di contatto principale per le questioni relative alla protezione dei dati personali e dovrebbe facilitare la comunicazione interna ed esterna sull'adempimento delle normative sulla Privacy.
L'Ordine Territoriale dei Medici Veterinari deve porre particolare attenzione al **Rapporto Annuale** sulla Conformità al GDPR redatto dal RPD a seguito delle attività di audit interni che sono state svolte, ed attivarsi a seguire le indicazioni contenute nel Rapporto per mantenere e/o migliorare l'efficacia delle misure di protezione dei dati e la conformità alle normative sulla Privacy.

ARTICOLO 10 - NOMINA DI RPD CONDIVISO

Gli Ordini Territoriali dei Medici Veterinari con numero di iscritti più limitati e risorse finanziarie ridotte potrebbero trovarsi in difficoltà nel nominare un Responsabile Protezione Dati con le caratteristiche e le capacità indicate dagli artt. 37, 38 e 39 del Regolamento UE 2016/679.
In particolare l'art. 37 par. 2 indica la possibilità di designare un unico Responsabile Protezione Dati (RPD) condiviso tra più organizzazioni (cosiddetto "RPD Condiviso"), a condizione che lo stesso sia facilmente accessibile da ciascuna di esse.
Questo significa che le organizzazioni, specialmente quelle che fanno parte di un unico organismo ed hanno strutture o funzioni simili, possono avere un RPD condiviso, a patto che la sua accessibilità e capacità di svolgere efficacemente i compiti richiesti dal GDPR non siano compromesse.
I compiti dell'RPD condiviso sono sostanzialmente gli stessi dell'RPD tradizionale.
Nel caso specifico degli Ordini Territoriali minori dei Medici Veterinari, l'adozione di un Codice di Condotta comune può costituire l'elemento determinante per valutare la possibilità di nomina di un RPD Condiviso.
Un RPD condiviso è un modello in cui più Ordini Territoriali di Medici Veterinari decidono di condividere un RPD per svolgere le loro funzioni di protezione dei dati.
In questo caso, il RPD condiviso può essere un individuo od anche un team di esperti che lavorano con più Ordini Territoriali, ciascuno dei quali è soggetto a obblighi di protezione dei dati, come è il caso degli Ordini Territoriali minori citati in precedenza.

Un RPD condiviso opera come punto di contatto comune per le organizzazioni coinvolte e svolge le stesse funzioni di un RPD tradizionale. La differenza sta nel fatto che il RPD condiviso deve essere in grado di gestire e soddisfare le esigenze di protezione dei dati di più organizzazioni contemporaneamente, coordinando e garantendo la conformità di tutte le parti coinvolte.
Il RPD tradizionale e il RPD condiviso devono possedere le competenze tecniche e professionali ed essere dotati delle risorse necessarie per svolgere le funzioni loro assegnate in modo efficace e indipendente. Il RPD deve essere in grado di mantenere la riservatezza e l'imparzialità nel trattamento dei Dati Personali.
La conoscenza della possibilità di effettuare questa scelta, attraverso sessioni formative in materia di Privacy organizzate per gli Ordini stessi, verrà promossa dagli Ordini Promotori.
Gli Ordini Territoriali cosiddetti Minori potranno comunque organizzarsi autonomamente tra di loro al fine di costruire una soluzione che garantisca loro la piena conformità al GDPR mediante l'utilizzo di un RPD condiviso.

ARTICOLO 11 - REGISTRO DEI TRATTAMENTI

L'art. 30 del GDPR prevede, tra gli adempimenti a carico del Titolare e del Responsabile del trattamento, la tenuta del **Registro delle Attività di Trattamento**.
Si tratta di documento, generalmente in forma tabellare su supporto cartaceo oppure elettronico, che contiene le principali informazioni relative alle operazioni di trattamento svolte dalla organizzazione; gli Ordini Territoriali dei Medici Veterinari, in quanto soggetti che effettuano Trattamenti a rischio (art. 30, par. 5), devono mantenere un registro delle attività di trattamento.
Sin dalla introduzione del Regolamento, è stato chiaro come esso costituisca uno dei principali elementi di accountability del Titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei Trattamenti posti in essere all'interno della propria organizzazione, ed indispensabile per ogni attività di valutazione o analisi del rischio, dunque preliminare rispetto a tali procedimenti.

Il Registro dei Trattamenti costituisce una irrinunciabile misura di accountability; come peraltro indicata all'art. 8 di questo Codice. La predisposizione e l'aggiornamento costante di un registro dei Trattamenti sono le fondamenta della protezione dei Dati Personali trattati dall'Ente.

L'aggiornamento del registro è essenziale: essendo un documento di censimento e analisi dei Trattamenti effettuati, il Registro deve essere mantenuto costantemente aggiornato e il suo contenuto deve sempre corrispondere all'effettività dei Trattamenti posti in essere. Qualsiasi cambiamento in ordine a modalità, finalità, categorie di dati, categorie di Interessati, deve essere riportato immediatamente nel registro,

motivando le modifiche adottate nel Trattamento: i cambiamenti adottati potrebbero infatti aver modificato il livello di rischio che incombe sui Dati Personali trattati. Pertanto occorrerà rivalutare, e contestualmente modificare, anche le misure di sicurezza adottate.

IL GDPR individua dettagliatamente le informazioni che debbono essere contenute nel Registro delle Attività di Trattamento (all'art.30 e al considerando 82); nel sito della Autorità sono disponibili approfondimenti ed indicazioni sul tema.
Il Registro dei Trattamenti deve essere esibito in occasione di ispezioni degli organismi competenti o a seguito di richieste della Autorità di Controllo.
Tra gli allegati del presente Codice di Condotta, è compreso un Registro dei Trattamenti di esempio, ricavato dalle attività di analisi svolte dal Gruppo di lavoro presso gli Ordini Territoriali dei Medici Veterinari Territoriali, che hanno collaborato alla creazione di questo Codice di Condotta.

ARTICOLO 12 - PROCEDIMENTI DISCIPLINARI

Le modalità per la gestione dei procedimenti disciplinari sono determinate dal D.P.R. 221/1950 e ss.mm.ll. a garanzia del rispetto del Codice Deontologico dei Medici Veterinari.
Il procedimento disciplinare è caratterizzato dalla necessità di scambio di informazioni e dati, compresi Dati Personali comuni e particolari (giudiziari).
Pertanto è richiesta una gestione cauta e sicura del trattamento dei Dati Personali, in linea con i principi di tutela chiaramente prescritti dal GDPR.
È opportuno che l'Ordine Territoriale definisca una specifica Procedura operativa atta a garantire una gestione corretta di tutte le fasi del procedimento disciplinare
Poiché l'esito del Procedimento Disciplinare ha talvolta rilevanza pubblica, è indispensabile che tutti i soggetti che si troveranno a dover trattare i Dati Personali relativi a questa procedura abbiano piena consapevolezza dei principi di:

1. Legalità, correttezza e trasparenza: il trattamento dei Dati Personali deve avvenire in modo lecito, corretto e trasparente nei confronti dell'interessato.
2. Limitazione delle finalità: i Dati Personali devono essere raccolti per scopi specifici, espliciti e legittimi, e non ulteriormente trattati in modo incompatibile con tali scopi.
3. Minimizzazione dei dati: i Dati Personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati.
4. Esattezza: i Dati Personali devono essere esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare senza ritardo Dati Personali inesatti rispetto alle finalità per cui sono trattati.
5. Limitazione della conservazione: i Dati Personali vanno conservati in una

forma che consenta l'identificazione degli Interessati per un periodo non superiore al conseguimento delle finalità per le quali i Dati Personali sono trattati.
6. Integrità e riservatezza: i Dati Personali devono essere trattati in modo da garantire un'adeguata sicurezza dei Dati Personali, ivi compresa la protezione, mediante misure tecniche e organizzative adeguate, da Trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danneggiamento accidentale. Sono suggerite misure di separazione dei dati relativi ai procedimenti disciplinari fisiche o logiche, adottando anche strumenti di cifratura dei dati.

Soprattutto per questo tipo di Trattamento dei Dati è opportuno che, nella specifica Procedura sopra suggerita che descrive le modalità di gestione del procedimento disciplinare, si ponga particolare attenzione a garantire che:

1. i Dati Personali siano trattati conformemente con le finalità stabilite per il procedimento disciplinare, in base a una appropriata base giuridica.
2. i diritti degli Interessati siano rispettati, tutelati da adeguate misure, inclusa la possibilità di esercitare, nei casi previsti, i diritti concessi dal GDPR (accesso, rettifica, cancellazione, limitazione del trattamento, opposizione al trattamento, portabilità dei dati).
3. le informazioni, relative al procedimento disciplinare e alle sanzioni applicate che sono destinate alla pubblicazione, devono necessariamente essere trattate ponendo particolare riguardo al bilanciamento della trasparenza e del diritto all'informazione pubblica con il rispetto della Privacy dei soggetti coinvolti. Queste informazioni devono essere esatte, aggiornate e non eccedenti rispetto alle finalità per le quali sono trattate. È opportuno che vengano adottate modalità di anonimizzazione per le informazioni personali, specialmente di terzi, non necessarie agli scopi.

Riguardo alla Comunicazione e Diffusione dei Dati relativi alla conclusione del Procedimento Disciplinare, le norme che regolano l'Albo prevedono diverse modalità di comunicare e diffondere a soggetti pubblici e privati le informazioni contenenti Dati Personali, compresi quelli contenuti nei provvedimenti di sospensione o interruzione dell'esercizio della professione.

Gli Ordini Territoriali devono quindi sempre avere cura di garantire che:

1. qualsiasi comunicazione o diffusione di Dati Personali rispetti i principi di proporzionalità e necessità;
2. tutte le informazioni pubblicate, sia cartacee sia con strumenti informatici e online, siano trattate con cura per evitare la diffusione di dati eccessivi e per garantire l'aggiornamento e la correttezza dei dati divulgati.

Nei Procedimenti Disciplinari il Responsabile della Protezione dei Dati (RPD) assume un ruolo fondamentale, non tanto nel singolo procedimento disciplinare, ma

nell'aver già in precedenza assicurato il rispetto della normativa di protezione dei Dati Personali da parte dell'Ordine Territoriale, minimizzando il rischio di non conformità e proteggendo i Dati Personali coinvolti.

In questo coinvolgimento il Responsabile della Protezione dei Dati (RPD) svolgerà le sue funzioni tipiche di:

1. Sorveglianza e Consulenza, monitorando la conformità dei procedimenti disciplinari con il GDPR;
2. Formazione e Sensibilizzazione, organizzando sessioni di formazione e sensibilizzazione per i membri dell'Ordine Territoriale coinvolti nei procedimenti disciplinari, per assicurarsi che comprendano le loro responsabilità sotto il GDPR.
3. Verifica della Conformità, tramite audit periodici per assicurare che i procedimenti disciplinari siano conformi al GDPR, verificando nel contempo che siano state implementate misure tecniche e organizzative adeguate per la sicurezza dei Dati Personali.
4. Consulenza su Risposte ai Diritti degli Interessati, fornendo consulenza su come gestire le richieste degli Interessati relativamente ai loro diritti sotto il GDPR (accesso, rettifica, cancellazione, opposizione al trattamento, ecc.) e assicurando che l'Ordine Territoriale risponda tempestivamente e in modo adeguato alle richieste degli Interessati.
5. Valutazione e Mitigazione dei Rischi, supportando l'Ordine Territoriale nelle decisioni relative alla divulgazione di informazioni sui procedimenti disciplinari al pubblico, assicurando che tali decisioni rispettino il principio di minimizzazione dei dati.

Adottando queste regole e coinvolgendo attivamente il Responsabile della Protezione dei Dati (RPD) nei procedimenti disciplinari, l'Ordine Territoriale dei Medici Veterinari può significativamente ridurre il rischio di violazioni dei Dati Personali trattati in relazione ai procedimenti disciplinari e tutelare efficacemente tutti i soggetti Interessati coinvolti nel procedimento.

ARTICOLO 13 - SUPPORTO ECONOMICO E ASSISTENZIALE

Nell'ambito delle attività di collaborazione instaurate dagli Ordini Territoriali dei Medici Veterinari con gli Enti Previdenziali (ad es. con l'ENPAV) l'Ordine Territoriale garantirà il rispetto delle normative vigenti in materia di protezione dei Dati Personali e della Privacy.
La tipologia dei dati trattati, che costituiscono **dati "particolari"** in quanto possono contenere anche indicazioni sullo stato di salute ed economico delle persone fisiche, richiede particolari attenzioni per garantire la loro protezione.

È necessario quindi garantire:

1. **Conservazione sicura dei dati:** i dati (cartacei e non) devono essere conservati in luoghi sicuri, ad esempio in armadi chiusi a chiave o su server protetti da password robuste e con accesso limitato solo al personale autorizzato.
2. **Crittografia dei dati sensibili:** è opportuno far ricorso alla crittografia per proteggere i dati sensibili durante la trasmissione e lo stoccaggio. Occorre quindi prevedere l'adozione di protocolli sicuri per l'invio di informazioni tramite internet e la crittografia dei dati archiviati.
3. **Accesso limitato e autorizzato:** solo le persone autorizzate possono accedere ai dati sensibili. Devono essere implementati controlli nell'accesso fisico ai luoghi di archiviazione, password complesse e/o l'uso di autenticazione a più fattori.
4. **Formazione del personale:** il personale coinvolto nel trattamento dei dati deve essere adeguatamente addestrato e sensibilizzato alla protezione dei dati particolari in modo sicuro e in conformità con le leggi sulla Privacy.
5. **Conformità normativa:** devono essere rigorosamente rispettate le leggi e i regolamenti sulla Privacy dei dati (GDPR), e assicurarsi che il trattamento dei dati sia conforme a tali normative.
6. **Monitoraggio e aggiornamento:** per individuare e rispondere prontamente a potenziali minacce alla sicurezza dei dati bisogna monitorare costantemente i sistemi informatici, mantenendo aggiornati i protocolli di sicurezza in modo da essere pronti ad affrontare i cambiamenti nelle minacce informatiche.
7. **Privacy by Design:** integrare la protezione dei dati fin dalla progettazione dei sistemi e dei processi per garantire che la sicurezza sia una considerazione fondamentale in ogni fase.

La protezione dei Dati Personali deve costituire per gli Ordini Territoriali dei Medici Veterinari un impegno continuo.

ARTICOLO 14 – WHISTLEBLOWING E PROTEZIONE DEI DATI

Nella gestione del Whistleblowing, cioè nella segnalazione, da parte di membri dell'Ordine o terzi, di attività sospette o illecite relative alla protezione dei dati personali, l'Ordine Territoriale garantirà il rispetto delle regole enunciate nel presente Codice di Condotta.
A tutela del Segnalante, il Trattamento dei Dati rispetterà i seguenti principi:

- Legalità, Correttezza e Trasparenza;
- Limitazione della Finalità;
- Minimizzazione dei Dati;
- Accuratezza;
- Limitazione della Conservazione;

- Integrità e Confidenzialità.

Saranno adottate tutte le misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al rischio del trattamento, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danno accidentale, utilizzando tecnologie avanzate e procedure rigorose di sicurezza.
L'Ordine Territoriale si doterà di una procedura informatica di gestione del Whistleblowing sicura ed accessibile per permettere ai segnalanti di riferire le irregolarità. Tale procedura dovrebbe essere preferibilmente accessibile dal sito dell'Ordine Territoriale, garantire l'anonimato del segnalante, se desiderato, e l'uso di strumenti di crittografia per proteggere la riservatezza delle informazioni trasmesse.

Occorre adottare misure per proteggere i Segnalanti da ritorsioni e per salvaguardare i diritti e le libertà degli Interessati, in conformità alle norme del GDPR.
La valutazione delle segnalazioni ricevute sarà fatta tempestivamente ed altrettanto tempestiva dovrà essere la relativa indagine. Nella misura in cui ciò non pregiudichi l'esito delle indagini e/o le misure di protezione o le indagini stesse, potranno essere fornite al Segnalante, se appropriato, informazioni dettagliate riguardanti l'esito delle indagini.
Verranno fornite informazioni chiare e accessibili riguardo alla procedura di whistleblowing, comprese le modalità di segnalazione e le garanzie previste per i Segnalanti e i soggetti Interessati, conformemente agli obblighi di trasparenza previsti dal GDPR.
I membri, i dipendenti e i collaboratori dell'Ordine saranno formati sulle procedure di whistleblowing, con particolare attenzione alla protezione dei dati personali e alla procedura di gestione delle segnalazioni.

ARTICOLO 15 - ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Le modalità per l'esercizio di tutti i diritti da parte degli Interessati sono stabilite, in via generale, negli artt. 12 e seguenti, del GDPR.
Per tutti i diritti il termine per la risposta è un mese, estendibile fino a tre mesi in casi di particolare complessità (dando comunque all'interessato comunicazione del motivo per cui viene estesa a tre mesi la risposta).
Il Titolare deve comunque dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego.
L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Spetta al Titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere, ma soltanto se si tratta di richieste manifestamente infondate, eccessive o anche ripetitive (art.12,

par. 5), o se sono chieste più "copie" dei Dati Personali nel caso del diritto di accesso (art.15, par. 3). In quest'ultima ipotesi, il Titolare deve tenere conto dei costi amministrativi sostenuti.
Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità. Può essere dato oralmente solo se lo richiede lo stesso interessato (art. 12, par. 1, e art. 15, par. 3).
È utile predisporre una procedura formalizzata di gestione delle istanze di esercizio dei diritti degli Interessati, efficace nel garantire il presidio di tutti i possibili canali di ricezione di tali istanze da parte di autorizzati al trattamento istruiti nel riconoscerle ed incardinarle secondo il canale più efficace a garantire una pronta e completa risposta.

ARTICOLO 16 - LA PROTEZIONE DEI DATI PERSONALI

Garantire la sicurezza dei dati è una misura essenziale di accountability.
In assenza di una efficace politica di sicurezza dei dati, non è possibile ottenere una reale protezione delle informazioni personali.
Oggi lo strumento elettronico è prevalente, ma sono sempre molto usati supporti cartacei; talvolta il dato personale co-esiste sia nel dominio digitale che in quello fisico, aumentando il livello di rischio che incombe sul dato stesso (i rischi a carico dei Trattamenti su supporti cartacei si sommano a quelli relativi ai duplicati elettronici).
Anche il concetto di **valutazione del rischio** è presente tra le misure di accountability.
La sua accorta gestione, consente di evitare potenziali incidenti e violazioni dei Dati Personali.
Nella normativa di protezione, la gestione del rischio è intesa come **cruscotto** indicatore del rischio dinamico che incombe sul trattamento; il livello del rischio è determinato da vari fattori, quali tipologia del dato personale, strumenti di trattamento adottati, ambiti operativi, flussi di comunicazione, trasferimenti vs. terzi, solo per indicarne alcuni.
Sebbene in qualsiasi attività reale il rischio zero sia impossibile da ottenere, ogni Titolare o Responsabile del Trattamento deve adottare misure organizzative, tecniche e logiche per **ridurre ad un livello accettabile** il rischio che incombe su ogni specifico trattamento posto in essere.
In generale si associa al concetto di sicurezza del dato la sicurezza informatica, trascurando il *dominio cartaceo*.
La sicurezza informatica non può **prescindere** dalla **sicurezza fisica**.
Molte validissime misure di protezione logica, largamente implementate per garantire la sicurezza informatica, perdono gran parte della loro reale efficacia qualora lo strumento elettronico cada nelle mani di un soggetto malevolo.
Si pensi alla protezione fornita dalle credenziali all'utente di un notebook, qualora il

dispositivo sia trafugato e sottoposto a procedure di "password reset" dell'account utente, oppure qualora si tentino – con tutta calma – procedure di "brute-force" della protezione crittografica adottata.

Cosa si intende per sicurezza informatica.
La sicurezza informatica interessa specificamente gli strumenti elettronici e le infrastrutture informative.
In questo codice di condotta consideriamo, come ambito di riferimento specifico, piccole realtà operative come gli Ordini Territoriali, che generalmente utilizzano, per i Trattamenti di Dati Personali, essenzialmente qualche personal computer o notebook, smartphone ed un collegamento dati per la connettività ad Internet.
Avendo quindi come riferimento questi ambiti operativi, riteniamo importante indicare le principali buone prassi operative da adottare per mantenere un elevato livello di sicurezza dei Trattamenti.

In primis, definiamo il concetto di sicurezza del dato come la condizione nella quale sono garantite la protezione, l'integrità e la riservatezza delle informazioni veicolate dal dato. Si tratta quindi di adottare misure atte a preservare i dati da accessi non autorizzati, modifiche indesiderate, perdite della confidenzialità e della integrità delle informazioni. Sicurezza del dato significa garantire che esso sia protetto da minacce (interne ed esterne alla organizzazione), come hacker, malware, perdita o furto di dispositivi o errori umani.

Una violazione dei dati non è esclusivo frutto di una debolezza di uno strumento elettronico o di un bug del software: di solito essa è correlata ad un comportamento non conforme o un errore umano, in genere per mancanza di consapevolezza.
A ben poco vale adottare i più sicuri protocolli di autenticazione, quando l'utente sceglie una password insicura; proprio per questo nella normativa di protezione è indicato l'obbligo di formare il personale, attività che viene approfondita nell'articolo 17.

16.1 Fonti di rischio nei Trattamenti cartacei ed elettronici e strategie di protezione

L'aspetto primario della protezione dei dati è conoscere le fonti di rischio; quindi occorre calcolarne il livello e ridurlo al minimo accettabile.
Avendo come riferimento gli **ambiti operativi predetti**, di seguito sono elencate le **principali fonti di rischio** per i Trattamenti nei due diversi domini, cartaceo ed elettronico.

Le fonti di rischio nei Trattamenti in formato cartaceo

Con riguardo ai Trattamenti di dati in formato cartaceo, fermo restando gli altri rischi (es. incendio, allagamento, infiltrazioni, …) gli aspetti più rilevanti da considerare sono la **riservatezza** e la **disponibilità** dei documenti contenenti Dati Personali.

Al fine di garantire riservatezza e disponibilità del dato personale su supporti cartacei, occorre:

- mantenere i documenti in appositi archivi, schedari o contenitori, chiusi a chiave;
- assicurare che solo le persone autorizzate abbiano accesso ai documenti contenti Dati Personali;
- prelevarli per le attività di trattamento, avendo cura che terzi non incaricati non possano accedervi;
- al termine delle attività di trattamento, riporre i documenti negli archivi;
- proteggere il trasferimento dei documenti, per esempio segregandoli in contenitori o tramite buste chiuse;
- a fine del loro ciclo di vita, distruggere i documenti in modo sicuro (distruggidocumenti).

Le fonti di rischio nei Trattamenti con strumenti elettronici

Per i Trattamenti svolti con strumenti elettronici, le fonti di rischio sono molteplici. Gli strumenti di trattamento elettronici considerati sono essenzialmente Personal Computer (PC), NoteBooks, SmartPhones e dispositivi di memoria rimovibili.
In molte realtà ordinistiche aventi struttura operativa di limitate dimensioni, sono impiegati solo un Notebook ed uno Smartphone, il quale spesso fornisce anche la connettività dati al Notebook.
Questa condizione determina che entrambi i **dispositivi mobili** sono contemporaneamente usati:

- per trattare Dati Personali;
- per le normali attività di office automation;
- per attività di navigazione e posta elettronica.

Con riguardo ai dispositivi elettronici descritti, le più importanti fonti di rischio derivano da:

- potenziale navigazione su eventuali siti web malevoli o compromessi da attori ostili;
- ricezione di e-mail con allegati contenenti malware o codice malevolo;
- collegamento di dispositivi di memoria rimovibile con codice malevolo;
- furto o smarrimento dei dispositivi mobili;
- vulnerabilità del software usato (sia del sistema operativo che degli applicativi);
- fulminazioni o irregolarità nella alimentazione elettrica.

Queste fonti di rischio possono compromettere la riservatezza, la disponibilità e l'integrità dei Dati Personali trattati negli strumenti indicati.

Misure per garantire la disponibilità dei dati

In relazione alla disponibilità del dato, la misura primaria da adottare è il salvataggio (backup) dei dati contenuti nei dispositivi, e questa è una misura di **semplice attuazione** e di **grande beneficio**. Esistono una molteplicità di soluzioni disponibili, sia per PC – NoteBooks che per SmartPhones. Occorre aver cura di mantenere i backup in un luogo diverso da quello operativo, onde evitare che un incendio o allagamento distrugga dispositivi e backup posti nello stesso luogo.
I backup dovrebbero essere automatici e registrare archivi in forma cifrata; periodicamente occorre effettuare **procedure simulate di ripristino** dei dati per verificare l'effettiva efficacia delle stesse.
Altra misura molto efficace è quella di adottare applicativi o servizi **in cloud**.
Un Cloud Provider adotta certamente avanzate procedure di backup interne, che sgravano la piccola realtà dal dover effettuare/verificare periodicamente backup di dati. Si consiglia di richiedere al cloud provider la disponibilità di uno strumento di esportazione che consenta comunque di trasferire periodicamente l'intero archivio dei dati in una unità di memorizzazione locale sicura.

Misure per garantire la riservatezza dei dati

Al fine di tutelare la riservatezza dei dati presenti negli strumenti elettronici, la prima misura è costituita dall'adozione di ***robuste*** credenziali di autenticazione al dispositivo. La ***robustezza*** della credenziale di autenticazione, qualora essa sia costituita semplicemente da "nome-utente + password", è determinata essenzialmente dalla complessità della password adottata, che deve essere complessa, non riconducibile all'utente e sostituita periodicamente.

Come seconda misura, tesa a **minimizzare il rischio di perdita della riservatezza** dei Dati Personali presenti nei dispositivi elettronici, in particolare quelli portatili (Notebooks, SmartPhones, PenDisks, ecc…), **in caso di smarrimento o furto**, è necessario cifrare i Dati Personali presenti nel device o unità di memoria.
Esistono molte valide soluzioni di crittografia, sia commerciali che open-source, semplici da usare, che rendono pressoché impossibile accedere ai dati cifrati a soggetti terzi che non dispongono delle chiavi di decifratura.
La cifratura protegge non solo i dati memorizzati nei filesystems, ma anche durante il loro trasferimento; è quindi necessario adottare protocolli di cifratura sia per invio e ricezione della posta elettronica che nel browser, quando con esso si trasferiscono Dati Personali, **specialmente in caso di dati particolari**.

Misure per garantire l'integrità dei dati

Un dato è considerato integro quando è completo, non è stato alterato o corrotto in

modo indesiderato, e rappresenta fedelmente l'informazione originale. Quindi mantenere l'integrità del dato è fondamentale per assicurare la sua protezione.
La prima misura per mantenere l'integrità dei dati registrati negli strumenti elettronici qualora essi siano soggetti a irregolarità della alimentazione elettrica, è costituito dalla adozione di un apposito UPS (Uninterruptible Power Supply) per proteggerli da variazioni di tensione, interruzioni di corrente o altre irregolarità nell'alimentazione elettrica. Si tratta di dispositivi comunemente disponibili e dal costo accessibile. È necessario controllare periodicamente lo stato delle batterie.
Una ulteriore misura a garanzia della integrità de dati consiste nel monitorare lo stato ed i parametri (SMART) delle unità di memorizzazione (HDD, SSD, ecc.), e sostituirle quando il loro *stato di salute* non sia più ottimale o i parametri siano al di fuori dei limiti di sicurezza.

Misure effetti di tutela con multipli su R-I-D.

Cosi come esistono dei vettori malevoli che vanno ad incidere su più di uno degli aspetti di sicurezza (Riservatezza, Integrità e Disponibilità), fortunatamente esistono anche delle misure di protezione che tutelano contemporaneamente più aspetti della sicurezza dei dati.
Per quanto riguarda i rischi derivanti dalla navigazione web e dalla ricezione di messaggi malevoli di posta elettronica, occorre premettere che gli attacchi informatici veicolati tramite navigazione o posta elettronica, come l'hacking, il phishing o il malware, possono compromettere l'integrità dei dati, consentendo agli attaccanti di alterare o corrompere i dati, ma anche renderli indisponibili ed addirittura esfiltrarli (es. nel caso di molte tipologie di ransomware). **Un unico vettore ostile compromette simultaneamente i tre aspetti della sicurezza IT**.
La principale contromisura da adottare è una valida soluzione di sicurezza del dispositivo (si tratta di software di protezione, comunemente detti antivirus, che oggi offrono protezione completa anche verso minacce di rete, ransomware, attacchi web, phishing, web-trackers, frodi informatiche, spam, vulnerabilità del software, ecc…).
A proposito del **codice malevolo**, è necessario ridurre al minimo la possibilità di essere eseguito sul dispositivo elettronico; questa misura di protezione è implementabile semplicemente utilizzando **account con privilegi ridotti** (di livello User - utente) al posto degli account con privilegi amministrativi (Administrator) che di default sono configurati negli OS Windows. Si tratta di una misura dal costo nullo ma di grande efficacia.
Per **ridurre la superficie di attacco** di PC e Notebooks, è consigliato disabilitare ogni servizio non utilizzato (per esempio, nei PC con OS Windows, di default è configurato il servizio di condivisione di file e stampanti, che nella maggior parte dei casi non è usato, e costituisce la porta di accesso ai vari malware che tentano di propagarsi in rete locale, tra i vari device che vi sono collegati).

Una ulteriore misura di protezione è costituita dalla formazione degli utilizzatori dei sistemi IT sui rischi, sulle corrette procedure da seguire e sui comportamenti da evitare (vedasi a proposito l'articolo 17 del presente Codice di Condotta).
Ove possibile, un livello maggiore di sicurezza è ottenibile trasferendo – in un diverso dispositivo dedicato – le attività di navigazione e di posta elettronica; si avranno pertanto due separati dispositivi, uno primario delegato esclusivamente al trattamento principale di Dati Personali ed un secondario, adibito alla esclusiva navigazione e gestione della posta elettronica (con relativo trattamento di tali dati).
Se correttamente configurati, un incidente al dispositivo secondario (navigazione + e-mail) non avrebbe ripercussioni sul primario (Trattamenti di Dati Personali più importanti o principali).

Amministratore di sistema e/o manutentore IT

La figura dell'Amministratore di Sistema (AdS, o System Administrator) ha un ruolo centrale nella protezione dei sistemi informatici; sono AdS le figure professionali che gestiscono e manutengono infrastrutture informative, sistemi operativi, software applicativi, reti di comunicazione e database. La figura dell'AdS è stata da tempo attenzionata nella normativa Privacy (provvedimento **"Misure e accorgimenti prescritti ai titolari dei Trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - 27 novembre 2008 e successive modifiche del 25 giugno 2009**).

Nel provvedimento figura assume una **estrema rilevanza** nella operatività e nella sicurezza delle infrastrutture informative. Per questo motivo è indispensabile che essa sia scelta previa una seria valutazione della esperienza, delle capacità e dell'affidabilità del soggetto selezionato; inoltre occorre prevedere misure per la verifica delle attività svolte sui sistemi amministrati.

Le attività svolte dall'AdS sono molto importanti per la sicurezza e continuità della infrastruttura ITC amministrata; ne riassumiamo solo alcune, le più rilevanti in questo contesto:

- gestione degli accessi degli utenti/incaricati al trattamento e adozione di vari livelli di accesso alle varie risorse ITC e programmi gestionali, onde consentire l'accesso alle informazioni minime necessarie per lo svolgimento delle attività conferite agli incaricati stessi;
- aggiornamenti, configurazioni e hardening continuo di sistemi, strumenti, dispositivi, software e misure di sicurezza, onde risolvere vulnerabilità, bug del software e configurazioni insicure (talvolta un config ritenuto sicuro, per rapidi mutamenti degli scenari, diviene insicuro);
- installazione e gestione dei software di protezione (anti-malware) e loro controllo;

- configurazione e monitoraggio della connettività verso InterNet e della LAN, valutazione e gestione del traffico dati e degli eventi di sicurezza;
- monitoraggio delle attività della infrastruttura, analisi dei log per individuare attività sospette; monitoraggio della integrità delle informazioni;
- salvataggio dei dati e ripristino, implementazione delle strategie di backup e test periodici di restore per valutarne l'efficacia;
- effettuazione di audit di controllo periodici sullo "stato di salute" di dispositivi e software, risoluzione di non conformità emerse.

Generalmente, nelle organizzazioni strutturate la figura dell'amministratore di sistema è svolta da un dipendente interno. Le ridotte dimensioni della infrastruttura IT e le esigue risorse disponibili di taluni Ordini Territoriali potrebbero rendere necessario esternalizzare tali attività.

A tale proposito, ricordiamo come la nomina di un amministratore di sistema sia stata oggetto di un provvedimento della Garante della Protezione dei Dati Personali nel 2008, che prescrive in particolare di valutare le caratteristiche soggettive della persona che andrà e rivestire il ruolo di AdS e la sua designazione individuale come persona fisica (e non della azienda della quale esso fa parte!). Nella designazione dell'AdS (se Esterno) si suggerisce di richiedere espressamente **modalità di accesso sicure** alla infrastruttura IT amministrata nel caso in cui l'attività venga svolta tramite connessione remota.

Gli aggiornamenti del software e del firmware

In generale, i programmi per computer (software) possono contenere errori di programmazione che potrebbero pregiudicare l'integrità dei dati (tramite essi) trattati. Il software contiene anche vulnerabilità che – se sfruttate da soggetti terzi malevoli – possono compromettere la sicurezza dell'intero dispositivo, quando non di tutta l'intera infrastruttura. È quindi importante che gli aggiornamenti del software siano effettuati frequentemente, onde porre rimedio prima possibile agli errori e/o alle vulnerabilità evidenziatesi nell'ultimo periodo. Gli aggiornamenti debbono essere effettuati sia per il sistema operativo (O.S.) sia per tutti i programmi presenti nel dispositivo usato per il trattamento dei Dati Personali.

Di conseguenza **non si possano usare**, per il trattamento di Dati Personali, software o sistemi operativi che non siano più aggiornabili (attualmente, per esempio, Windows 7, 8, 8.1 in quanto EOL – End Of Life), cosi come gli applicativi non più aggiornabili (esempio, Office 2007, 2010, 2013).
Con riguardo al firmware (si tratta di uno speciale software che fa funzionare dispo-

sitivi elettronici come stampanti, router, NAS, ed in generale tutti i dispositivi informatici diversi dai computer) esso va mantenuto sempre aggiornato, in quanto anche una stampante di rete vulnerabile può costituire un "cavallo di Troia" che aggressori esterni possono usare per compromettere tutta la rete locale. Analogamente il firmware del firewall va mantenuto esente da vulnerabilità, in quanto esso costituisce il primo baluardo dalle aggressioni che sono portate dall'esterno verso la rete locale.

Le verifiche di sicurezza

In ottemperanza al punto d) dell'Art. 32 GDPR, periodicamente vanno effettuate procedure di verifica della efficacia delle misure di sicurezza adottate.
Esse debbono riguardare:

- la effettività delle procedure di salvataggio, effettuando simulazioni di ripristino dei backups;
- la corretta funzionalità del software di protezione;
- lo stato dell'aggiornamento dei software nei sistemi;
- la ricerca della eventuale presenza di vulnerabilità negli strumenti elettronici;
- la resilienza di servizi informatici erogati su InterNet (es. il sito web o il server di posta elettronica).

Periodicamente occorre sottoporre i dispositivi a controlli di sicurezza, quali verifiche degli eventi occorsi (registri di Windows o log di sistema), alla ricerca di errori e operazioni di log-in fallite oppure anomalie nelle attività.
È necessario che i servizi IT particolarmente esposti a rischi e/o gli strumenti di sicurezza (es. il firewall che regola i flussi da e verso Internet) siano sottoposti a prove (cd. Penetration Test) per capire il livello di ***resilienza*** che garantiscono. Tali controlli sono anche tesi a rilevare errori nelle configurazioni, oppure impostazioni di sicurezza non adeguate al livello di rischio gravante (per esempio, l'utilizzo di protocolli di cifratura deprecati o poco sicuri).

Garantire la sicurezza dei Trattamenti di Dati Personali non è una attività una-tantum, bensì di un processo reiterante, con il quale si valuta costantemente il rischio incombente sui Trattamenti e si adotta le adeguate contro-misure.

La maggior parte degli incidenti Privacy deriva da comportamenti errati degli operatori (il c.d. fattore umano): per questo motivo la formazione di tutte le persone delegate al trattamento dei dati e l'aumento della loro consapevolezza diventano elementi essenziali per aumentare il livello della sicurezza dell'Ordine Territoriale.

ARTICOLO 17 - FORMAZIONE DEGLI INCARICATI

La formazione degli incaricati - adesso autorizzati al trattamento - rappresenta uno dei fondamenti nella costruzione di una cultura aziendale basata sulla protezione dei dati. Essa contribuisce in modo significativo a rappresentare la accountability aziendale nei confronti della protezione dei dati.

La formazione non è un mero adempimento normativo, ma va intesa quale opportunità per accrescere la consapevolezza degli incaricati sui principi fondamentali della protezione dei Dati Personali e migliorare l'interazione con tutti coloro che conferiscono i loro Dati Personali. Attraverso la formazione si promuove un approccio collaborativo e trasparente verso gli Interessati, rafforzando la loro fiducia nel modo in cui trattiamo i loro Dati Personali e dimostrando il nostro impegno a essere responsabili nel loro utilizzo.
Inoltre, un impegno costante nella formazione e nel rispetto della normativa Privacy permette alle realtà di migliorare la loro reputazione e crescere come organizzazione Responsabile e consapevole della protezione dei Dati Personali.

Nel seguito indichiamo, a titolo indicativo e non esaustivo, alcuni temi che possono essere affrontati nella formazione degli autorizzati:

- **Introduzione alla Protezione dei Dati Personali:**
  concetti di base legati alla protezione dei Dati Personali, inclusi i principi fondamentali del GDPR;
- **Concetto di dato personale:**
  dato personale; differenze tra dati comuni e dati particolari.
- **I principi fondamentali del trattamento dei Dati Personali:**
  - legittimità, trasparenza e finalità del trattamento;
  - minimizzazione dei dati: raccogliere solo i dati necessari;
  - limitazione della conservazione: conservare i dati solo per il tempo necessario;
  - integrità e riservatezza dei dati;
- **Ruoli e Responsabilità:**
  definizione dei ruoli e delle responsabilità degli incaricati del trattamento, compresi i loro doveri specifici;

- **Normativa sulla Privacy:**
  un'analisi di dettaglio della normativa Privacy vigente, con enfasi particolare sui principali articoli del Regolamento GDPR, e degli eventuali provvedimenti particolarmente rilevanti per l'organizzazione;
- **Le informative sulla Privacy:**

cosa debba contenere l'informativa, come debba essere fornita in modo esauriente ed efficace ai soggetti Interessati;

- **Consenso e Revoca:** il consenso e la revoca del consenso;
- **Le Basi Legali per il Trattamento:**
  basi legali che giustificano il trattamento dei Dati Personali;
- **Gestione dei Dati Personali:**
  le procedure adottate per la raccolta, l'elaborazione, la conservazione e la distruzione dei Dati Personali in conformità con la normative in vigore;
- **Sicurezza dei Dati:**
  le misure di sicurezza fisiche, logiche ed organizzative adottate per proteggere i Dati Personali; le best practices ed esempi di problematiche da evitare;
- **Notifica delle Violazioni dei Dati:**
  il concetto di violazione, tipologie ed effetti; la gestione del Data Breach e gli obblighi di segnalazione alle autorità competenti ed eventualmente alle persone interessate.
- **Casi pratici ed esempi:**
  le casistiche ricorrenti, le misure preventive e le best practices procedurali.
- **Il regolamento per il corretto uso degli strumenti e dei servizi interni:**
  scopi, indicazioni e limitazioni;
- **Formazione Continua:**
  aggiornamento continuo, migliori pratiche in materia di protezione dei dati;
- **Verifica delle competenze:**
  valutazione del grado di formazione raggiunto; procedure per valutare il livello generale di conoscenza della normativa degli addetti al trattamento.

Una formazione degli autorizzati, correttamente effettuata ed aggiornata nel tempo, specialmente quando intervengano mutamenti rilevanti degli strumenti di trattamento o dei ruoli svolti da essi, rappresenta un passo essenziale per garantire un trattamento responsabile e conforme delle informazioni personali.

ARTICOLO 18 - GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

La normativa di protezione dei Dati Personali richiede di gestire il livello di rischio che grava sui Trattamenti, riducendolo ad un livello accettabile, nella consapevolezza che il rischio zero non è ottenibile nelle attività reali.
Pertanto, ad ogni Titolare o Responsabile del trattamento è richiesto di adottare preventive misure organizzative, logiche e tecniche per minimizzare il rischio; ciononostante, il livello residuale di rischio **potrebbe comunque determinare un evento avverso** sui dati trattati denominato, nel GDPR, violazione dei Dati Personali.

Per violazione dei Dati Personali, o Data Breach nella terminologia inglese, si intende "*ogni violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati*".
Nel Data Breach quindi vengono meno una o più caratteristiche intrinseche della sicurezza dei dati, la riservatezza, l'integrità o la loro disponibilità.
Viene meno la riservatezza quando avviene un accesso non autorizzato alle informazioni personali, come nei casi di un soggetto esterno non titolato che acceda ai sistemi.
Le violazioni dei Dati Personali possono verificarsi in diverse circostanze e possono avere origini sia interne che esterne all'organizzazione.
Di seguito, analizziamo alcune casistiche in grado di determinare un Data Breach:

- **Accesso non autorizzato o hacking**: quando un attaccante esterno riesce a violare i sistemi informatici o le reti dell'organizzazione e ottiene l'accesso non autorizzato ai Dati Personali; questo può determinarsi da vulnerabilità nel software, phishing, attacchi di tipo ransomware o altre tecniche di hacking.
- **Furto o smarrimento di dispositivi**: qualora un dispositivo contenente Dati Personali venga smarrito o rubato, ad esempio un NoteBook, uno smartphone o una chiavetta USB, ai Dati Personali presenti sul dispositivo potrebbero avere accesso terzi non titolati, con le conseguenze che potrebbero anche essere ulteriormente diffusi ad altri soggetti.
- **Errore umano**: errori umani, come ad esempio inviare per errore informazioni personali a persone sbagliate, pubblicare Dati Personali in modo non protetto o modificare dati senza esservi autorizzati.
- **Insicurezza delle credenziali di accesso**: l'utilizzo di credenziali deboli o la condivisione non autorizzata di password può rendere più facile per gli attaccanti accedere illecitamente ai sistemi IT e quindi ai Dati Personali in essi presenti.
- **Furto o accesso da parte di dipendenti infedeli**: in alcuni casi, dipendenti interni possono rubare o accedere in modo improprio ai Dati Personali dei clienti o dei colleghi.
- **Vulnerabilità dei sistemi**: I sistemi informatici vulnerabili o malconfigurati, proni a intrusioni di malintenzionati, consentono loro di compromettere o esfiltrare i dati.
- **Malfunzionamento tecnico**: problemi tecnici, difetti hardware o errori nei sistemi informatici possono portare a cancellazioni, perdite della integrità o esposizioni di Dati Personali.
- **Attacchi interni**: dipendenti o collaboratori potrebbero compiere azioni dannose intenzionalmente, per ritorsioni o estorsioni.

- **Violazioni da parte di fornitori o partner**: le violazioni possono verificarsi anche attraverso fornitori o partner esterni con i quali l'organizzazione ha condiviso Dati Personali, oppure qualora siano installati software di terze parti che siano vulnerabili o contengano backdoor di accesso non documentate.
- **Mancanza di controlli e politiche di sicurezza**: un'organizzazione potrebbe non avere in atto adeguati controlli di sicurezza o politiche per proteggere i Dati Personali, aumentando per questo il rischio di violazioni.
- **Denial of Service (DoS) o Distributed Denial of Service (DDoS)**: Gli attacchi DoS o DDoS possono causare la temporanea interruzione dei servizi o del sistema, rendendo i Dati Personali inaccessibili o esposti.

Effetti della violazione dei dati sulle persone Interessate.

Una violazione dei Dati Personali rappresenta una minaccia effettiva per la Privacy e la sicurezza delle persone alle quali tali dati si riferiscono; le violazioni dei dati possono avere un impatto significativo sulla vita delle persone coinvolte.

Nel seguito sono alcuni effetti avversi generati agli Interessati da un Data Breach:

- **Rischio di Furto d'Identità:**
  Le informazioni personali esposte in una violazione dei dati possono essere utilizzate per il furto d'identità, causando gravi danni personali, oppure conseguenze legali, come la necessità di dimostrare la propria innocenza in caso di attività fraudolente;
- **Rischi finanziari:**
  i dati finanziari possono essere compromessi, portando a transazioni non autorizzate o a frodi finanziarie;
- **Violazione della riservatezza**:
  gli Interessati possono soffrire della violazione della loro Privacy e per la divulgazione non autorizzata delle loro informazioni personali, specialmente qualora i dati affetti siano di natura particolare;
- **Impatto sulla Reputazione degli Interessati**:
  le persone possono sperimentare la perdita o il deterioramento della propria reputazione personale, specialmente se alcune informazioni sensibili diventano pubbliche a causa del Data Breach.
- **Potenziale perdita del posto di lavoro:**
  qualora siano coinvolti i loro dati professionali o particolari, gli Interessati potrebbero affrontare problemi sul posto di lavoro, deterioramento delle relazioni con i colleghi, ivi compresa la perdita del lavoro o la necessità di abbandonarlo.

- **Impatto Emotivo:**
  le persone coinvolte possono sperimentare stress, ansia e preoccupazioni per la loro sicurezza e Privacy, specialmente se il data-breach ha coinvolto Dati Personali molto rilevanti; purtroppo abbiamo visto come in alcuni casi le persone siano state portate ad atti estremi.

Gestione Tempestiva delle Violazioni dei Dati

Le violazioni dei dati devono essere gestite in modo tempestivo ed efficace, essendo la tempestività determinante per limitarne gli effetti avversi:

- **Limitare i danni a carico delle persone coinvolte**:
  una risposta rapida può aiutare a limitare i danni causati dalla violazione, ad esempio bloccando tempestivamente l'accesso non autorizzato ai dati o ai sistemi oppure cambiando la password di accesso ai servizi on-line;
- **Conformità Normativa**:
  Il GDPR richiede la notifica dal Data Breach alla autorità Garante per la Protezione dei Dati Personali entro 72 ore dal momento nel quale se ne è avuta conoscenza; inoltre, qualora la violazione comporti un rischio elevato per i diritti e le libertà degli Interessati, è fatto obbligo al Titolare di comunicare anche agli Interessati che i loro Dati Personali sono stati oggetto di una violazione.
- **Preservare la Fiducia**:
  una risposta tempestiva dimostra impegno nella protezione dei dati e può contribuire a preservare la fiducia degli Interessati;
- **Ridurre il Rischio Legale**:
  una gestione Responsabile può ridurre il rischio di azioni legali da parte degli Interessati o delle autorità di controllo.

Un Data Breach ha un **impatto diretto sulle persone coinvolte** e richiede una risposta rapida e responsabile per limitare i danni ed azionare contromisure atte a proteggere la Privacy e la sicurezza degli Interessati, in ambiti non ancora toccati dalla violazione.
La gestione delle violazioni dei Dati Personali deve essere considerata un elemento essenziale nella strategia globale di protezione dei dati di qualsiasi organizzazione. Per affrontare queste situazioni con la massima serietà ed urgenza, è fondamentale che le organizzazioni si dotino, in anticipo, di procedure consolidate per la gestione delle violazioni dei Dati Personali. Sarebbe altresì importante predefinire il team delle persone delegate alla sua gestione.

Procedura per la gestione della violazione di Dati Personali

Identificazione

La prima fase è la identificazione della violazione; a tal fine occorre aver predisposto strumenti di monitoraggio, atti a rilevare eventuali violazioni. Parimenti, è fondamentale aver istruito gli incaricati al trattamento sugli eventi che possano far pensare ad un Data Breach. In tale ambito, la **formazione** è fondamentale. Gli incaricati devono essere consapevoli che omettere le segnalazioni di eventi anomali al referente Privacy o al RPD potrebbe avere conseguenze gravi, sia a carico degli Interessati sia della stessa organizzazione.

Isolamento

La seconda fase consiste nel prendere tempestivamente tutte le misure per impedire l'aggravarsi del Data Breach, contemporaneamente adottando le accortezze per non alterare lo stato dei sistemi oggetto di violazione; in genere, una violazione determina anche effetti giuridici, per cui dovranno essere espletate attività di indagine e giudiziarie. In genere, si disabilitano i servizi compromessi o si disattivano (si spegne il server).

Valutazione dell'accaduto

Una fase essenziale è la valutazione di quanto accaduto, cercando di comprendere le modalità, il grado di violazione e di conseguenza il rischio associato alla violazione; occorre considerare la natura dei dati coinvolti, il numero di Interessati, il possibile impatto e le potenziali conseguenze sulle persone potenzialmente derivanti dalla violazione. Questo è necessario anche per determinare i prossimi passi da compiere.

Notifica alle Autorità Competenti

"Senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, si deve notificare la violazione al Garante per la Protezione dei Dati Personali a meno che sia improbabile che la violazione dei Dati Personali comporti un rischio per i diritti e le libertà delle persone fisiche". Quindi la notifica al Garante non viene fatta solamente nel caso in cui sia **assolutamente improbabile** che la violazione **comporti un rischio**, anche minimo, a carico delle persone oggetto di violazione.

In generale la notifica deve essere fatta tempestivamente, comunque entro 72 ore, indicando tutto quanto sino adesso conosciuto; successive informazioni ed analisi approfondite potranno essere fornite all'Autorità di Controllo con successive ulteriori notifiche. Si segnala come sia determinante predisporre tempestivamente la documentazione richiesta dalla Autorità di Controllo e mantenere una comunicazione costante con la stessa.

Notifica agli Interessati

Qualora la violazione possa rappresentare un rischio significativo, anche se solo potenziale, per gli Interessati, è necessario segnalarlo, con modalità ritenute appropriate, direttamente agli Interessati.
Occorre fornire informazioni chiare sulla natura della violazione, sulle azioni intraprese e sulle misure che gli Interessati possono adottare per limitare gli effetti della violazione.

Mitigazione e Recupero
A seguire, occorre intraprendere le azioni immediate volte a mitigare i danni, in particolare quelli che derivano dalla eventuale indisponibilità del dato; questo non prima però di aver risolto la causa del breach, per esempio nei casi in cui siano state usate credenziali compromesse (che debbono essere disattivate) oppure vulnerabilità (che debbono essere prima risolte).
In genere per il ripristino della operatività si azionano le procedure di restore (**disaster recovery**). Si consiglia di registrare accuratamente tutte le azioni effettuate. Certamente è importante avere a supporto aziende esperte in tali scenari di ripristino.

Analisi delle Cause e Reportistica
Al fine di identificare le cause del Data Breach occorre condurre un'indagine interna approfondita per determinare le cause della violazione, inclusa l'identificazione delle vulnerabilità o delle lacune nei processi. Si dovrà anche preparare un report dettagliato sulla violazione, sulle azioni intraprese e sulle misure correttive adottate per prevenire future violazioni.

Comunicazione e Relazioni Pubbliche
Nei casi in cui occorra, si dovranno preparare comunicati stampa e dichiarazioni pubbliche, per comunicare in modo trasparente ed efficace con gli Interessati, partner commerciali ed in generale verso l'opinione pubblica. In tale scenario, sarebbe necessario il supporto di professionisti, cosi come di un supporto legale.

Archiviazione della documentazione
Tutta la documentazione, relativa alla violazione e alle azioni intraprese per dimostrare la conformità alle leggi sulla Privacy, dovrà essere conservata accuratamente per il periodo richiesto dalla normativa.

Rivedere ed aggiornare procedura e misure di sicurezza
Qualora si verifichi un Data Breach, sarà opportuno analizzare le misure adottate al fine di comprendere che cosa non abbia funzionato. Quindi si dovranno rivedere, migliorare ed aggiornare le misure di sicurezza, anche eventualmente adottandone di nuove o implementandone di migliori. Inoltre occorre sempre rivedere la procedura

di gestione dei Data Breach per tenerla allineata alle evoluzioni delle leggi e delle minacce informatiche. Nell'analisi post-incidente è sempre necessario coinvolgere il team di gestione dei Data Breach per identificare miglioramenti e memorizzare la lezione appresa.

ARTICOLO 19 - USO DEI SOCIAL MEDIA

Nell'attuale contesto digitale, qualunque sia la professione che si intende svolgere, non si può prescindere dall'uso, o quantomeno dalla conoscenza, dei mezzi di comunicazione digitale. Le tecnologie digitali, infatti, hanno cambiato per tutti il modo di informarsi, ma anche il modo di promuovere la professione. I social network, ad esempio, nonostante le problematiche ad essi connessi - dal loro uso eccessivo alla vulnerabilità di sicurezza online - sono ormai strumenti ampiamente inclusi nelle strategie commerciali di aziende e professionisti.

Di seguito alcuni suggerimenti per utilizzare in modo proficuo i social media per la promozione delle proprie attività.

Il primo step è dotarsi delle competenze digitali necessarie per partecipare alla società dell'informazione, senza avere la pretesa di essere degli esperti informatici. Superare il gap digitale significa sapere utilizzare gli strumenti a disposizione, senza rinunciare allo spirito critico. Occorre anche andare oltre certi pregiudizi, come quello di rifiutare a priori i social network perché magari considerati futili: i dati confermano che gli utenti delle piattaforme social crescono di anno in anno ed è chiaro che ormai non sono solo una moda ma uno stile di vita e di relazione, e che non possono essere ignorati.

A maggior ragione il discorso vale per gli Ordini Territoriali dei Medici Veterinari che, per la natura del lavoro che svolgono, sono comunque chiamati ad interessarsi degli effetti dannosi legati all'uso dei social network.
Oltre alle competenze digitali di base, vanno poi considerate quelle più specificatamente comunicative e di relazione, considerato che proporsi in rete richiede un'attenzione particolare al linguaggio; e che si può raggiungere un pubblico molto vasto e sconosciuto.

Ecco alcuni suggerimenti:

- Occorre assicurare la qualità dei contenuti. Non basta solo "postare" ma produrre informazioni di qualità, poiché questo significa accrescere "il proprio brand", distinguendosi così da altri professionisti.

- La comunicazione deve essere chiara e comprensibile per l'utenza cui ci si rivolge.
- È necessario conoscere le differenze tra i diversi tipi di social, al fine di scegliere quello che fa al caso proprio (anche più di uno): se ad esempio Linkedin nasce già come rete di business, frequentato soprattutto da aziende e professionisti che così promuovono il loro lavoro, Facebook, lanciato con un intento socializzativo è andato via via aderendo ad una logica anche professionale, potendo contare su una vastità di utenti.
- È altamente consigliabile tenere separata la propria vita privata da quella lavorativa sui profili social: se da un lato ne consegue un'immagine squisitamente professionale, dall'altro si riducono i rischi di sovrapporre i due livelli.
- Gli Ordini Territoriali dei Medici Veterinari che utilizzano i social devono essere consapevoli degli effetti che la comunicazione ha sull'utenza. Questo significa assumersi la responsabilità di ciò che si pubblica.
- I profili devono essere monitorati e aggiornati, altrimenti si rischia di dare l'impressione di "trascuratezza". Chi si rivolgerebbe ad un Ordine Territoriale dei Medici Veterinari che non ha cura di come si presenta agli altri?

Fra gli adempimenti Privacy, si consiglia che l'Informativa contenga l'indicazione:

- dell'eventuale utilizzo dei canali social distinti per tipo;
- dell'eventuale attività di digital marketing;
- del consenso per le attività di profilazione.

ARTICOLO 20 - MESSAGGISTICA ISTANTANEA

L'uso della messaggistica istantanea, tramite dispositivi mobili, rappresenta indubbiamente uno strumento agile e immediato per la comunicazione tra gli Ordini Territoriali e i loro Iscritti. Questa modalità di comunicazione può facilitare lo scambio di informazioni, fornire risposte rapide a dubbi o preoccupazioni, e soddisfare una vasta gamma di esigenze in modo tempestivo. Tuttavia, è fondamentale non trascurare l'importanza della protezione dei dati personali, in particolare considerando che nella messaggistica istantanea potrebbero confluire informazioni particolari sensibili come dati sanitari, dati giudiziari o dati finanziari degli Iscritti. Questi dati personali richiedono una protezione aggiuntiva ai sensi del GDPR.
Si raccomanda agli Ordini Territoriali un uso responsabile della Messaggistica Istantanea, attenendosi alle seguenti raccomandazioni:

1. **valutare i rischi per la privacy e la sicurezza delle informazioni,** prima di utilizzare strumenti di messaggistica istantanea per comunicare dati particolari.

2. preferire **l'uso di piattaforme di messaggistica che offrono cifratura end-to-end** e che sono conformi alle normative sulla protezione dei dati personali.
3. adottare il **principio di minimizzazione**, trasmettendo solo i dati strettamente necessari per il caso specifico, evitando la condivisione di informazioni non pertinenti o eccessive.
4. garantire una **adeguata formazione ai Soggetti Autorizzati** relativamente alle pratiche di sicurezza dei dati e alle implicazioni legali dell'uso della messaggistica istantanea.
5. informare gli Iscritti sulle politiche di Privacy relative all'uso della messaggistica istantanea, ottenendo il loro **consenso esplicito all'uso di tali canali** per la comunicazione di dati particolari.
6. **monitorare regolarmente l'uso** degli strumenti di messaggistica istantanea e rivedere le pratiche in atto per garantire la conformità continua con il GDPR e la protezione efficace dei dati personali.
7. **Utilizzare esclusivamente strumenti nella disponibilità dell'organizzazione ed evitare utilizzo di strumenti personali di dipendenti o componenti dell'Ordine.**

ARTICOLO 21 - SITO WEB DELL'ORDINE TERRITORIALE

Il sito web di una organizzazione costituisce la porta d'accesso primaria per informare e dare servizi a visitatori ed associati. La sua realizzazione non è solo una questione di design e funzionalità, ma anche di conformità normativa e sicurezza.
Nel seguito indicheremo le buone prassi da adottare ed i requisiti minimi per la realizzazione del sito web di un Ordine Territoriale dei Medici Veterinari Provinciale, in modo da assicurare la sua conformità alla normativa vigente, la sua sicurezza e funzionalità, offrendo quindi uno strumento solido per lo svolgimento dell'attività statutaria e le interazioni con utenti ed associati.
Ogni Ordine Territoriale dei Medici Veterinari deve quindi tutelare al meglio i Dati Personali dei visitatori del proprio sito web, ed è tenuto a seguire le regole di conformità alla complessa normativa di protezione, al fine di assicurare un trattamento sicuro e trasparente dei Dati Personali.
Come prima indicazione vorremmo soffermarci sulla scelta degli *attori in campo*; in genere un sito web è *ospitato* presso un hosting provider, e realizzato da un soggetto con competenze di informatica, oppure una web agency. La scelta di questi due players è fondamentale, in quanto su di essa si basa anche una determinante parte della tutela dei dati trattati tramite il sito web.
È quindi necessario basare la scelta non solamente su meri aspetti economici, ma soprattutto sulla scelta di partner tecnologici adeguati a garantire la sicurezza del

trattamento; questa forte indicazione proviene dal concetto stesso di **accountability** del Titolare del trattamento, che deve adottare infrastrutture e strumenti adeguati. Sempre in questa fase è necessario ricordarsi dei concetti di **Privacy by design e by default**, i quali determinano la necessità di integrare misure di protezione dei dati, sin da prima di costruire il sito web; e ricordarsi di limitare al minimo necessario, per il corretto svolgimento del trattamento progettato, le acquisizioni dei Dati Personali.
Occorre concentrare l'attenzione sul concetto di Profilazione, cioè sul processo attraverso il quale un sito web raccoglie e analizza attivamente informazioni su un utente, come ad esempio le sue preferenze, interessi, comportamenti di navigazione e altri Dati Personali. Queste informazioni consentono la creazione di un profilo dettagliato dell'utente al fine di offrirgli contenuti, pubblicità e/o servizi personalizzati in base alle caratteristiche e ai comportamenti individuati.
Le Web Agency sono particolarmente esperte nell'utilizzo degli strumenti di profilazione ed inevitabilmente portano il Cliente all'introduzione (a volte in modo anche inconsapevole) di meccanismi di profilazione all'interno del sito.

È opinione del Gruppo di Lavoro che ha collaborato alla stesura del presente Codice di Condotta che la Profilazione degli utenti del sito web non rientri tra le attività primarie di un Ordine Territoriale dei Medici Veterinari e quindi non sia necessario utilizzare nel sito istituzionale dell'Ordine Territoriale cookies di profilazione.

Gli aspetti negativi derivanti dall'uso della profilazione nel sito web dell'Ordine Territoriale, **di gran lunga superiori ai presunti vantaggi attesi**, si possono così riassumere:

1. violazione della Privacy;
2. rischi per la sicurezza;
3. manipolazione e discriminazione;
4. filtraggio dell'informazione;
5. creazione di profili errati o distorti;
6. abuso delle informazioni personali.

Per mitigare questi pericoli, si renderebbero necessarie regolamentazioni adeguate, trasparenza nell'uso dei Dati Personali, consenso informato degli utenti e misure di sicurezza per proteggere le informazioni raccolte durante il processo di profilazione. Tutto questo rappresenta un costo aggiuntivo che non sempre viene evidenziato dai fornitori al momento della proposta di realizzazione del sito web.

Come indicazioni generali, in relazione all'Hosting Provider potremmo menzionare la presenza di certificazioni di sicurezza (es. il framework ISO/IEC 2700x), mentre la web agency dovrebbe dimostrate competenza ed affidabilità nella predisposizione del codice informatico (html, javascript, php, ecc.) che *erogherà* il sito web.

Spesso le agenzie web sono molto competenti in merito alla parte informatica, ma meno preparate nella parte di compliance Privacy: per questo motivo molti siti non sono corredati da una adeguata informativa Privacy del sito ed anche non sono sempre conformi alla normativa sull'uso dei cookies.

Per gestire le funzionalità del sito, ma **soprattutto per la sua sicurezza**, è fondamentale la scelta della piattaforma CMS (Content Management System: lo strumento software che facilita la creazione e la gestione dei contenuti web).

La cronaca da tempo ci dimostra come un sito web male impostato, poco manutenuto, non aggiornato e soprattutto non costantemente monitorato, sia facile bersaglio di attacchi di terzi malintenzionati, anche se non dotati di particolari competenze.

Nel seguito vengono indicate le caratteristiche essenziali che dovrebbe avere il sito web di un Ordine Territoriale dei Medici Veterinari.

Informativa sulla Privacy
Il sito web dell'Ordine Territoriale dei Medici Veterinari deve fornire un'informativa sul trattamento dei Dati Personali degli utilizzatori del sito che sia accessibile, trasparente e comprensibile a tutti. Tale informativa dettaglia quali Dati Personali vengono raccolti, come vengono utilizzati, dove sono localizzati, con chi vengono condivisi e per quanto tempo verranno conservati; occorre prestare attenzione alla limitazione dei tempi di conservazione, specialmente per i dati provenienti dai log del webserver.

Cookies ed altri Strumenti generanti Identificativi
Da tempo in Italia vige una complessa normativa che regola l'uso di strumenti software generanti identificativi (cookies) ed altri strumenti di tracciamento. Alcuni di questi strumenti, di prima parte e quindi meno intrusivi, possono essere adottati senza consenso, mentre altri, denominati di terza parte, sono spesso utilizzabili ed utilizzati per tracciare gli utenti, e debbono essere **posti sotto consenso**. Si tratta del *fastidioso* pannello di gestione dei cookies che si propone quasi sempre ad ogni apertura di una pagina di un nuovo sito.
Il sito web **deve essere conforme a questa normativa** (la cosiddetta "cookie law") e quindi indicare in modo adeguato e preciso nell'informativa quali cookie sono utilizzati dal sito.

Diritti degli Interessati
Il GDPR concede agli Interessati un ventaglio di diritti (agli artt, 15 e successivi), per i quali essi possono accedere ai propri Dati Personali; li possono modificare; nei casi previsti ne possono richiederne copia o cancellazione.

Sicurezza dei Dati

Non è questo il luogo per affrontare il tema della sicurezza dei siti web in modo esaustivo. Nel seguito, considerando le finalità di questo Codice di Condotta, indicheremo i principali elementi di sicurezza che dovrebbero caratterizzare il sito web di un Ordine Territoriale dei Medici Veterinari:

- **adottare la cifratura della connessione server-client (https)** tramite l'impiego di appositi protocolli crittografici e di una infrastruttura PKI di chiavi crittografiche; questo consente di proteggere la comunicazione tra il web server ed il browser dell'utente.
- identificare e risolvere le vulnerabilità che si determinano a carico dei software utilizzati (C.M.S. e suoi plug-ins, web server, php, OS sottostante ecc.);
- impostare misure di autenticazione forte, attuando politiche di controllo degli accessi, password complesse e politiche di blocco account da accessi ripetutamente falliti;
- monitorare i logs del webserver per evidenziare e rispondere ad attività sospette;
- eseguire backup giornalieri e verificare l'effettività delle procedure sia di backup che soprattutto di restore;
- valutare, qualora il sito sia molto trafficato e/o soggetto ad attacchi, l'utilizzo di strumenti a contrasto e/o protezione, quali WAF (Web Application Firewalls) e CDN (Content Delivery Networks);
- formare la consapevolezza dell'importanza della sicurezza negli amministratori e negli utenti del sito.

Trasferimenti Internazionali di Dati Personali

Nel caso in cui i Dati Personali vengano trasferiti al di fuori dell'Unione Europea, dovranno essere state preventivamente adottate adeguate misure di sicurezza e clausole di garanzie per ottenere un livello di protezione equiparabile a quello offerto dal Regolamento Europeo; inoltre, gli utenti dovranno essere informati (tramite l'informativa presente nel sito) su tali trasferimenti. Qualora siano scelti componenti software generanti identificativi, occorre ricordarsi che molti di questi componenti determinano Trattamenti di Dati Personali extra-UE (prevalentemente negli USA, come per Google Analytics, i vari plug-in social-media, ecc.).

Violazioni dei Dati

Devono essere state **predefinite** chiare procedure per gestire e notificare eventuali violazioni dei Dati Personali, in conformità con la normativa di protezione vigente; si consiglia anche di predisporre il team di gestione data-breach.

Informazioni obbligatorie da indicare nel sito

Nel sito web debbono essere presenti i contenuti obbligatori, quali la identificazione della organizzazione, il link alla pagina dell'Ordine Territoriale presso il sito web della Federazione Nazionale, gli estremi di contatto del referente Privacy, le informazioni legali ed amministrative, le note legali, i termini e le condizioni di uso del sito. Qualora l'Ordine Territoriale abbia aderito a questo codice di condotta, è opportuno che tale adesione sia indicata anche nel sito web. Tra le informazioni obbligatorie rientrano anche gli estremi di contatto del RPD.

Si raccomanda anche di indicare la data dell'ultimo aggiornamento dei contenuti del sito, una pratica utile a mostrare trasparenza e a facilitare l'utente nella consultazione.

Estremi di contatto del RDP

L'Ordine Territoriale dei Medici Veterinari, che è tenuto alla designazione del Responsabile della Protezione dei Dati (RPD o DPO), deve indicare nel sito web ed in ogni informativa le specifiche informazioni di contatto del RPD, a beneficio degli utenti che desiderano contattarlo per ricevere informazioni o proporre istanze inerenti ai propri Dati Personali. L'indirizzo di posta elettronica – assolutamente dedicato e non condiviso - del RPD (es rpd@ordineprovincialeXX.it) è indicato nei contatti generali del sito web e nelle Informative Privacy e cookies.

Aggiornamenti del Sito Web

Il sito web dell'Ordine Territoriale dei Medici Veterinari dovrà essere sottoposto a regolari revisioni per garantirne la conformità con il GDPR e con le normative più recenti in materia di protezione dei dati.

Periodicamente occorre anche far eseguire assessments di sicurezza sul sito web, condotti da realtà terze qualificate.

ARTICOLO 22 MODALITÀ DI ADESIONE AL CODICE DI CONDOTTA

L'adesione al presente Codice di Condotta è aperta a tutti gli Ordini Territoriali dei Medici Veterinari che desiderino impegnarsi nel rispetto delle disposizioni del GDPR e delle linee guida definite nel Codice.

L'adesione al Codice di Condotta è su base volontaria
L'Ordine Territoriale provvederà ad ottenere dal Consiglio dell'Ordine stesso la deliberazione formale indicante la volontà di adottare e implementare le disposizioni del Codice di Condotta all'interno della propria organizzazione.
L'Ordine invierà quindi una richiesta formale di adesione al Codice di Condotta all' Ordine Capofila del Progetto, indicando la volontà di adottare e implementare le disposizioni del Codice all'interno del proprio Ente, accompagnandola con la documentazione attestante l'avvenuta approvazione da parte del Consiglio dell'Ordine e l'impegno ad aderire a tutte le misure necessarie per conformarsi al Codice di Condotta.
L'Ordine Capofila fornirà la propria risposta entro trenta giorni dal ricevimento, motivando l'eventuale rifiuto.

L'adesione al Codice di Condotta per gli Ordini Territoriali dei Veterinari è gratuita.

Si ricorda a tutti gli Ordini Territoriali che la semplice dichiarazione di adesione al Codice di Condotta non è di per sé elemento sufficiente a garantire la conformità dell'Ente ai principi del Regolamento Europeo sulla Protezione dei Dati Personali (GDPR).
Quindi nell'aderire al Codice di Condotta occorrerà considerare, oltre al **"costo di adesione"**, anche i cosiddetti **"costi di conformità"** cioè quei costi che sarà necessario sostenere per adeguarsi ai requisiti specifici del codice di condotta. Ciò potrebbe comportare la revisione dei processi interni, la formazione del personale o l'implementazione di nuovi sistemi per garantire la conformità al GDPR.

ARTICOLO 23 - VERIFICHE SUL RISPETTO DEL CODICE DI CONDOTTA

Ogni Ordine Territoriale dei Medici Veterinari, avvalendosi della collaborazione del proprio Responsabile della Protezione dei Dati Personali, adotta apposite procedure di controllo documentato sull'osservanza del Codice.

Il controllo, affidato a un soggetto terzo indipendente, verrà svolto con cadenza almeno annuale e i relativi i report saranno conservati dal Responsabile della Protezione dei Dati Personali per almeno cinque anni.

Il Garante per la protezione dei dati personali, nel rispetto delle indicazioni degli articoli da 56 a 58 del Regolamento, effettua le opportune verifiche del rispetto del presente Codice di condotta da parte del Titolare.

ARTICOLO 24 - REVISIONE DEL CODICE E DISPOSIZIONI TRANSITORIE E FINALI

I 19 Ordini Territoriali dei Medici Veterinari, che ne sono stati i promotori attivi, sottoscrivono il presente Codice di Condotta per gli Ordini Territoriali dei Medici Veterinari.

Il Gruppo di lavoro, istituito dagli Ordini Promotori, ha svolto numerosi incontri con gli Ordini Territoriali e gli iscritti agli Ordini Territoriali dei Medici Veterinari per analizzare le principali criticità riscontrate nell'applicazione delle norme del GDPR.
Il presente Codice di Condotta è il frutto della condivisione delle esperienze e delle competenze emerse in questi incontri nei vari soggetti che vi hanno partecipato.
Dal momento di inizio dei lavori il testo del Codice di Condotta è stato oggetto di numerose discussioni, condivisioni e modifiche.
Prima della presentazione al Garante per la Protezione dei Dati Personali, questo Codice di Condotta è stato presentato agli Ordini Territoriali durante il Consiglio Nazionale della FNOVI in data 20/aprile/2024 e quindi sottoposto a Pubblica Consultazione per un periodo di trenta giorni mediante:

- pubblicazione sul sito istituzionale pubblicazione sul sito istituzionale dell'Ordine Capofila del Progetto (https://ordineveterinari.va.it/codici-di-condotta/);
- invio a tutti gli Ordini Territoriali interessati (cento) mediante nota prot. N. 359 del 05/dicembre/2024, da parte dell'Ordine Capofila;

La versione che sarà presentata per l'approvazione al Garante per la Protezione dei Dati Personali verrà integrata con le osservazioni pervenute, al termine della pubblica consultazione, dai diversi soggetti interessati ed anche di quelle emerse nell'ambito degli incontri con i portatori di interesse coinvolti nella pubblica Consultazione.

ARTICOLO 25 ENTRATA IN VIGORE

Il presente Codice di Condotta, dopo l'approvazione da parte dell'Autorità Garante per la Protezione dei Dati Personali, verrà inserito nei registri di cui all'art. 40, paragrafi 6 e 11, del Regolamento, e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana, acquistando efficacia il giorno successivo a quello della pubblicazione.

Il Codice di Condotta può essere soggetto a modifiche in caso di aggiornamenti successivi all'entrata in vigore che dipendano da cambiamenti di natura normativa e/o regolatoria e/o della prassi e degli usi nel settore di riferimento.

RICONOSCIMENTI

Il progetto rientra fra quelli approvati con i fondi destinati al "Bilancio partecipativo" della Federazione Nazionale.

Il Progetto è stato promosso e sostenuto dagli Ordini Territoriali dei Medici Veterinari di Agrigento, Brindisi, Catania, Chieti, Como e Lecco, Cremona, Isernia, L'Aquila, Mantova, Messina, Novara, Pescara, Pordenone, Potenza, Taranto, Trento, Treviso, Varese e Vicenza.

Hanno collaborato alla definizione di questo Codice di Condotta:

GRUPPO DI LAVORO ESTERNO per la progettazione e lo sviluppo del Codice:

- dott. Giuseppe Giuliano;
- avv. Monica Gobbato;
- dott. Claudio Mazzucchelli;
- dott. Stefano Rossi;
- dott.ssa Loredana Sardo.

GRUPPO DI LAVORO INTERNO per la validazione/revisione del Codice:

- dott. Benedetto Neola;

ORDINE TERRITORIALE VETERINARI MILANO:

- Marina Pagliaro

ORDINE TERRITORIALE VETERINARI VARESE:

- Gabriella Bonetti
- Dott. Maurizio Mazzucchelli

RAPPRESENTANTI STRUTTURE VETERINARIE:

- dott. Daniele Alberti
- dott. Alessandro Guglielmo Aspesi
- dott.ssa Chiara Fulvia Recalcati

Le funzioni di segreteria sono state svolte dalla sig.ra Gabriella Bonetti.

Varese, 16 marzo 2024

ALLEGATI

ALLEGATO 1

Esempio di Informativa ai Medici Veterinari

esempio di Informativa dei trattamenti. I dati inseriti sono a titolo indicativo e non esaustivo

INFORMAZIONI DA FORNIRE ALL'INTERESSATO

Informazioni riguardanti il trattamento dei dati personali da fornire all'interessato ai sensi degli articoli 13 del regolamento (UE) 2016/679 rispettivamente, nel caso in cui le informazioni siano raccolte o meno presso l'interessato

Trattamento:
GE52 - Gestione Iscritti

Data: aprile 2024
Versione: 1.0

PROGETTO CODICE CONDOTTA ORDINI PROVINCIALI
Via dell'Ordine Provinciale - 12345 Città dell'Ordine Provinciale - Italia

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

DATI RACCOLTI PRESSO L'INTERESSATO

(ex art. 13 GDPR 2016/679)

Gentile interessato,

scopo del presente documento è di informare la persona fisica (secondo la normativa definito come "**interessato**") relativamente al trattamento dei dati personali raccolti dal titolare del trattamento Ordine Medici Veterinari della Provincia di CODICECONDOTTA (di seguito anche "**titolare**"), ai sensi dell'articolo 13 del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito anche "**Regolamento**" o "**GDPR (General Data Protection Regulation)**") e del D.Lgs. 2003/196 come modificato dal D.Lgs. 2018/101 "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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 anche "**Codice**").

Il titolare potrà modificare, in tutto o in parte, la presente informativa dandone comunicazione agli interessati.

I suoi dati personali saranno trattati secondo i principi di correttezza, liceità e trasparenza. La disponibilità, la gestione, l'accesso, la conservazione e la fruibilità dei dati è garantita dall'adozione di misure tecniche ed organizzative ritenute adeguate dal titolare del trattamento per assicurare gli opportuni livelli di sicurezza ai sensi degli articoli 25 e 32 del regolamento (UE) 2016/679 in riferimento alla propria attività.

Con riferimento ai dati personali oggetto di trattamento, il titolare fornisce le seguenti informazioni.

GENERALITÀ DEL TITOLARE DEL TRATTAMENTO E DATI DI CONTATTO

Il titolare del trattamento dei suoi dati personali è **Ordine Medici Veterinari della Provincia di CODICECONDOTTA**, con sede in Via dell'Ordine Provinciale - 12345 Città dell'Ordine Provinciale - Italia, responsabile nei suoi confronti del legittimo e corretto uso dei suoi dati personali e che potrà contattare per qualsiasi informazione o richiesta ai seguenti recapiti:

Telefono: 01234567890; Fax: 01234567890; E-mail: segreteria@ordineveterinari.cc.it; PEC: ordinevet.cc@pec.fnovi.it

CATEGORIE DI DATI PERSONALI TRATTATI

I suoi dati personali trattati dal titolare afferiscono alle seguenti categorie di informazioni:

Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Deposito firma su registro consegna timbro professionale tondo; Stato di salute

FINALITÀ DEL TRATTAMENTO

I suoi dati personali sono raccolti e trattati per le finalità riportate di seguito insieme al criterio sul quale si fonda il trattamento e all'eventuale base giuridica di riferimento:

Finalità	Criterio di liceità	Categorie di dati trattati	Basi giuridiche
Cura dei rapporti con gli assistiti	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.)	Esecuzione di un contratto

CATEGORIE PARTICOLARI DI DATI PERSONALI

Tra le categorie di dati oggetto del trattamento rientrano informazioni classificate come particolari e disciplinate dall'Art. 9 del Regolamento (sensibili, genetici, biometrici, relativi alla salute, ecc.). In particolare, i dati che la riguardano appartengono alle seguenti categorie: Stato di salute.

Il trattamento dei dati personali appartenenti a tali categorie particolari è possibile poiché fondato sulle condizioni seguenti:

Condizione	Descrizione
Finalità di medicina preventiva o di medicina del lavoro	

MODALITÀ DI TRATTAMENTO E COMUNICAZIONE DEI DATI

Il trattamento sarà svolto in forma manuale, nel rispetto di quanto previsto dall'art. 32 del GDPR 2016/679 in materia di misure di sicurezza, ad opera di soggetti appositamente incaricati e in ottemperanza a quanto previsto dall'art. 29 GDPR 2016/ 679.

Il Titolare adotta le opportune misure di sicurezza volte ad impedire l'accesso, la divulgazione, la modifica o la distruzione non autorizzate dei Dati Personali.

Il trattamento viene effettuato mediante strumenti informatici e/o telematici, con modalità organizzative e con logiche strettamente correlate alle finalità indicate. Oltre al Titolare, in alcuni casi, potrebbero avere accesso ai dati altri soggetti coinvolti nell'organizzazione aziendale (personale amministrativo, commerciale, marketing, legali, amministratori di sistema) ovvero soggetti esterni (come fornitori di servizi tecnici terzi, corrieri postali, hosting provider, società informatiche, agenzie di comunicazione) nominati anche, se necessario, Responsabili del trattamento da parte del Titolare. L'elenco aggiornato dei Responsabili potrà sempre essere richiesto al Titolare del trattamento.

DESTINATARI

In nessun caso i suoi dati saranno oggetto di divulgazione a destinatari, come definiti all'articolo 4 del regolamento (UE) 2016/679.

PERIODO DI CONSERVAZIONE

I dati sono trattati e conservati per il tempo strettamente richiesto dalle finalità per le quali sono stati raccolti.

In linea generale, i dati personali raccolti per scopi collegati all'esecuzione di un contratto tra il titolare e l'interessato saranno trattati sino a quando sia completata l'esecuzione di tale contratto; i dati personali raccolti per finalità riconducibili all'interesse legittimo del titolare saranno trattati sino a quando sussisterà tale legittimo interesse.

Quando il trattamento è basato sul consenso dell'interessato, il titolare può conservare i dati personali fino a quando detto consenso non venga revocato.

Inoltre, il titolare potrebbe essere obbligato a conservare i dati personali per un periodo maggiore di quello inizialmente stabilito per ottemperare a un obbligo di legge o per ordine di un'autorità pubblica.

Al termine del periodo di conservazione i dati personali saranno cancellati. Pertanto, successivamente a tale termine i diritti di accesso, cancellazione, rettifica e alla portabilità dei dati non potranno più essere esercitati da parte dell'interessato.

La tabella seguente contiene informazioni dettagliate riguardanti il criterio seguito per determinare la conclusione del ciclo di vita dei dati e/o la presumibile data di conclusione e/o il periodo prestabilito del loro trattamento.

Trattamenti	Descrizione
- Gestione Iscritti (GE52 - Gestione Iscritti attivi;	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)
GE52 - Gestione Iscritti (GE52 - Gestione Iscritti)	I dati fanno parte dell'archivio storico dell'Ordine. I datii sono conservati in un apposito contenitore e rimangono a disposizione dell'Ordine per verifiche per tutta la durata della permanenza dell'associato nell'Ordine. L'Ordine tiene uno storico di tutti gi Albi annuali a tempo indeterminato in apposito armadio chiuso a chiave

TRASFERIMENTO DEI DATI PERSONALI

I suoi dati non saranno trasferiti in Paesi terzi non appartenenti all'Unione Europea o verso organizzazioni internazionali non stabilite nel territorio dell'Unione.

DIRITTI DELL'INTERESSATO

Oltre alle informazioni sopra riportate, per garantire un trattamento dei suoi dati personali più corretto e trasparente possibile, è opportuno che sia a conoscenza del fatto che in ogni momento potrà esercitare, ai sensi degli articoli dal 15 al 22 del regolamento (UE) 2016/679, il diritto di:

a) chiedere l'accesso ai dati personali e la conferma dell'esistenza o meno di propri dati personali;

b) ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione;

c) ottenere la rettifica e la cancellazione dei dati;

d) ottenere la limitazione del trattamento;

e) ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad un altro titolare del trattamento senza impedimenti;

f) opporsi al trattamento in qualsiasi momento e anche nel caso di trattamento per finalità di marketing diretto;

g) opporsi ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione;

h) revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

i) proporre reclamo a un'autorità di controllo.

Può esercitare i suoi diritti con richiesta scritta inviata via posta tradizionale o via email ai recapiti indicati in questo documento.

Firma del Titolare del Trattamento e data
Ordine Medici Veterinari della Provincia di CODICECONDOTTA
Xx aprile 2024

_____

ALLEGATO 2

Esempio di nomina di Soggetto Autorizzato

Il sottoscritto **ORDINE VETERINARIO ABCDE**, Titolare del Trattamento dei dati personali ai sensi del Regolamento UE 2016/679 in materia di protezione delle persone fisiche,

CONSIDERATO CHE

È necessario attuare la migliore qualità conseguibile nel trattamento dei dati personali e ciò è possibile attuando in piena autonomia la gestione dei compiti del proprio ufficio
Risulta necessario configurare la propria struttura secondo criteri di efficienza e efficacia, delegando compiti operativi a personale che possieda abilità e formazione opportune per svolgere le mansioni a esso delegato
A seguito di apposita attività conoscitiva e valutativa è risultato che ***SOGGETTO AUTORIZZATO*** offre garanzie sufficienti circa le proprie qualità professionali e personali, in particolare esperienza, capacità e affidabilità nella conoscenza della base normativa (Regolamento UE 2016/679, D.Lgs. 2003/196) e delle prassi in materia di protezione dei dati personali, nonché della capacità di assolvere i compiti con scrupolosità e diligenza

NOMINA

SOGGETTO AUTORIZZATO, quale Persona Autorizzata (art. 4 Regolamento UE 2016/679 e art. 2 quaterdecies D.Lgs. 2003/196) per i trattamenti riportati di seguito insieme alle caratteristiche peculiari quali la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati e i permessi accordati:

Trattamento	**GE02 - Gestione Clienti**
Durata	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni), salvo nel caso di azione legale in corso per la quale i dati saranno mantenuti sino alla conclusione dell'azione legale. Data di inizio del trattamento: 01/01/2020
Natura	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.)
Finalità	Gestione della clientela
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti

Trattamento	**GE04 - Contabilità**
Durata	10 anni a decorrere dalla data di cessazione dei contratti con clienti e fornitori (art. 2220 codice civile che prevede la conservazione per 10 anni delle scritture contabili; art. 22 del D.P.R. 29 Settembre 1973, n.600) Data di inizio del trattamento: 01/01/2020
Natura	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Attività economiche, commerciali, finanziarie, assicurative
Finalità	Tenuta dei registri contabili; Adempimenti fiscali
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti; Personale dipendente; Fornitori; Consulenti e liberi professionisti, anche in forma associata

Trattamento	**SP08 - Reception**
Durata	Trattamento con durata prestabilita pari a 5 Anni Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Professione dichiarata
Finalità	Monitoraggio delle persone che fanno ingresso in azienda; Filtraggio delle telefonate
Tipo di dati personali	Dati comuni
Categorie di interessati	Consulenti e liberi professionisti, anche in forma associata; Fornitori; Potenziali clienti; Clienti o Utenti

Trattamento	**SA01 - Segreteria medica**

Durata	Trattamento con durata prestabilita pari a 5 Anni Data di inizio del trattamento: 01/01/2020
Natura	Origini razziali; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Tessera sanitaria; Stato di salute - patologie attuali; Stato di salute - terapie in corso; Sesso m/f; Stato di salute; Dati genetici; Dati biometrici; Dati di contatto (numero di telefono, e-mail, ecc.)
Finalità	Registrazione pazienti e gestione amministrativa
Tipo di dati personali	Dati sensibili; Dati comuni; Dati relativi alla salute; Dati genetici; Dati biometrici
Categorie di interessati	Clienti o Utenti; Familiari dell'interessato; Pazienti; Minori in condizioni di disagio sociale; Soggetti con patologie psichiche; Alunni disabili o in condizioni di disagio sociale

Trattamento	**AZ04 - Accettazione**
Durata	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni) Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale
Finalità	Accettazione delle merci
Tipo di dati personali	Dati comuni
Categorie di interessati	Fornitori

Trattamento	**AZ05 - Bollettazione e DDT**
Durata	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni) Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale
Finalità	Spedizione delle merci
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti

Trattamento	**GE22 - SpedizioneReferti-Documenti Fiscali**
Durata	I dati relativi alle singole spedizioni saranno eliminati dagli archivi della Azienda dopo due anni dalla spedizione. I responsabili esterni sono tenuti invece alla cancellazione dei dati dei destinatari entro due mesi dalla data di verifica dell'avvenuta consegna e non potranno utilizzare in alcun modo i dati di cui sono venuti a conoscenza. Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.)
Finalità	Gestione della clientela
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti

Trattamento	**YY02 - Gestione Corrispondenza - E-mail**
Durata	10 anni a decorrere dalla data di cessazione dell'ultimo evento scaturito dall'ultimo rapporto contrattuale in essere, a meno che non sia in corso un contenzioso legale, nel qual caso il periodo di conservazione dei dati non può essere stabilito a priori. Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale; Indirizzo e-mail; Lavoro (occupazione attuale, precedente, curriculum, ecc.)
Finalità	Gestione della clientela; Gestione del personale; Adempimenti in materia di protezione dei dati personali
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti; Potenziali clienti; Personale dipendente; Consulenti e liberi professionisti, anche in forma associata; Stagisti; Visitatori sito web

Trattamento	**YY05 - Gestione delle Telefonate**
Durata	Trattamento con durata prestabilita pari a 2 Anni Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Dati di contatto (numero di telefono, e-mail, ecc.); Argomenti di interesse; Ruolo ricoperto in azienda; Dati inerenti situazioni giudiziarie civili, amministrative, tributarie

Finalità	Gestione della clientela; Gestione del personale; Adempimenti in materia di protezione dei dati personali
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti; Potenziali clienti; Personale dipendente; Consulenti e liberi professionisti, anche in forma associata; Stagisti; Visitatori sito web

Trattamento	**SA12 - Emergenza Covid-19 (Green Pass)**
Durata	I dati trattati nell'ambito del controllo della certificazione verde CoViD-19 non saranno registrati né conservati. Data di inizio del trattamento: 15/10/2021
Natura	Nominativo, indirizzo o altri elementi di identificazione personale; Certificazione sanitaria a seguito del possesso di specifici requisiti
Finalità	Prevenzione dal contagio da COVID-19; Prevenzione dal contagio da COVID-19
Tipo di dati personali	Dati comuni; Dati relativi alla salute
Categorie di interessati	Personale dipendente; Lavoratori autonomi; Consulenti e liberi professionisti, anche in forma associata; Agenti e rappresentanti; Fornitori

Trattamento	Permessi accordati
YY05 - Gestione delle Telefonate	Lettura, Inserimento, Modifica, Stampa
YY02 - Gestione Corrispondenza - E-mail	Lettura, Inserimento, Modifica, Stampa
AZ04 - Accettazione	Tutti i Permessi
SA12 - Emergenza Covid-19 (Green Pass)	Lettura
GE02 - Gestione Clienti	Tutti i Permessi
SA01 - Segreteria medica	Tutti i Permessi
SP08 - Reception	Tutti i Permessi
AZ05 - Bollettazione e DDT	Tutti i Permessi
GE04 - Contabilità	Tutti i Permessi
GE22 - SpedizioneReferti-Documenti Fiscali	Tutti i Permessi

La persona autorizzata si impegna a:

- garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli e a non divulgare, neanche dopo la cessazione dell'incarico di Persona Autorizzata, alcuna delle informazioni di cui è venuto a conoscenza nell'adempimento dei compiti assegnatigli, sia perché connesso con tali attività che per caso fortuito (art. 28 par. 3 lettera b Regolamento UE 2016/679)
- ove applicabile, rispettare l'obbligo di riservatezza in ottemperanza alle norme deontologiche caratteristiche della professione esercitata secondo le norme vigenti (art. 28 par. 3 lettera b Regolamento UE 2016/679)

Comune, 02/01/20xx

Firma del Titolare del Trattamento
ORDINE VETERINARIO ABCDE

Con la firma in calce a tale documento accetto la nomina a **Persona Autorizzata** per i trattamenti prima riportati insieme alle loro caratteristiche peculiari

Firma della Persona Autorizzata
SOGGETTO AUTORIZZATO

_____

Ove applicabile, il presente documento annulla e sostituisce ogni altro documento di nomina a Persona Autorizzata di **RAVASINI LAURA** , già esistente e sottoscritto

Firma del Titolare del Trattamento
ORDINE VETERINARIO ABCDE

_____

Firma della Persona Autorizzata
SOGGETTO AUTORIZZATO

_____

ALLEGATO 3

Esempio di nomina di Responsabile Esterno

CONTRATTO PER LA NOMINA DEL RESPONSABILE DEL TRATTAMENTO

(ex art. 28 GDPR 2016/679)

Tra

ORDINE TERRITORIALE ABCDE, Titolare del Trattamento dei dati personali ai sensi del Regolamento UE 2016/679 in materia di protezione delle persone fisiche

E

RESPONSABILE ESTERNO, Partita IVA: 123456789012 – via del Fornitore 12345 Comune (XX) IT

OGGETTO

Ai sensi dell'art. 28 Regolamento UE n. 679/2016 e considerato che sussistono i requisiti di esperienza, capacità e affidabilità, **RESPONSABILE ESTERNO** viene nominato nella qualità di responsabile del trattamento per i trattamenti di dati personali di seguito riportati insieme alle caratteristiche peculiari quali la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati:

Trattamento	**TC02 - Manutenzione Software di Base**
Durata	Il Trattamento termina alla fine del Contratto: i dati saranno mantenuti per 5 anni dal termine del contratto, salvo gli obblighi di legge Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale; Codice fiscale ed altri numeri di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Natura dei beni; Valore dei beni; Certificati di qualità professionali
Finalità	Assistenza utenti
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti; Fornitori

Trattamento	**TC12 - Manutenzione Hardware**
Durata	Il Trattamento termina alla fine del Contratto: i dati saranno mantenuti per 5 anni dal termine del contratto, salvo gli obblighi di legge Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale; Codice fiscale ed altri numeri di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Natura dei beni; Valore dei beni; Certificati di qualità professionali
Finalità	Assistenza utenti
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti; Fornitori

Trattamento	**YY02 - Gestione Corrispondenza - E-mail**
Durata	10 anni a decorrere dalla data di cessazione dell'ultimo evento scaturito dall'ultimo rapporto contrattuale in essere, a meno che non sia in corso un contenzioso legale, nel qual caso il periodo di conservazione dei dati non può essere stabilito a priori. Data di inizio del trattamento: 01/01/2020
Natura	Nominativo, indirizzo o altri elementi di identificazione personale; Indirizzo e-mail; Lavoro (occupazione attuale, precedente, curriculum, ecc.)
Finalità	Gestione della clientela; Gestione del personale; Adempimenti in materia di protezione dei dati personali
Tipo di dati personali	Dati comuni
Categorie di interessati	Clienti o Utenti; Potenziali clienti; Personale dipendente; Consulenti e liberi professionisti, anche in forma associata; Stagisti; Visitatori sito web

OBBLIGHI DEL RESPONSABILE

Il Responsabile del Trattamento si impegna (art. 28 par. 3 Regolamento UE 2016/679) a:

- trattare i dati personali soltanto su istruzione documentata del Titolare del Trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in questa

circostanza il Responsabile del Trattamento informa tempestivamente il Titolare del Trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- assistere il titolare del trattamento con misure tecniche e organizzative adeguate, tenendo conto della natura del trattamento e nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- in particolare, qualora il responsabile tratti dati oggetto di richiesta di portabilità, si obbliga ad assistere il titolare del trattamento con misure tecniche e organizzative adeguate al fine di rispondere a detta richiesta;
- assistere il titolare del trattamento nel garantire il rispetto dell'obbligo di notifica di una violazione dei dati personali all'autorità di controllo di cui all'art. 33 e 34 Regolamento UE 679/2016. In caso di violazione dei dati personali il responsabile del trattamento informa il titolare senza ingiustificato ritardo e comunque entro il termine di 12 ore dal momento in cui è venuto a conoscenza della violazione;
- assistere il titolare del trattamento nelle attività relative alla valutazione di impatto sulla protezione dei dati e consultazione preventiva (artt. 35, 36 Regolamento UE 2016/679), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

MISURE DI CONTROLLO

RESPONSABILE ESTERNO si impegna a mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente accordo. Contribuisce alle attività di revisione, ispezioni e audit realizzati dal titolare del trattamento o da altro soggetto da questi incaricato.

MISURE TECNICHE E ORGANIZZATIVE

RESPONSABILE ESTERNO si impegna ad adottare ogni misura tecnica ed organizzativa adeguate per soddisfare quanto previsto dal Regolamento UE n. 679/2016 e garantire la tutela dei diritti dell'interessato.

- si impegna ad adottare le misure di sicurezza espressamente previste all'art. 32 Reg. UE n. 679/2016.

- In particolare, si impegna a osservare le disposizioni che vengono impartite dal Titolare, ad attuare gli obblighi di informativa e di acquisizione del consenso nei confronti degli interessati, nonché di assistere tempestivamente gli interessati che presentino richieste inerenti l'esercizio dei loro diritti informando tempestivamente il Titolare del trattamento di tali richieste.

- predispone e aggiorna un sistema di sicurezza adeguato.

- si attiene solo ai trattamenti previsti dal presente contratto, salvo che in presenza di obblighi di legge.

- provvede alla **nomina** del/i proprio/i **Amministratore/i di Sistema**, in adempimento a quanto previsto dal provvedimento del Garante della Privacy del 27.11.08, pubblicato in G.U. n. 300 del 24.12.2008, ove ne ricorrano i presupposti, curando, altresì, l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento.

SUB RESPONSABILI

Il responsabile del trattamento si impegna a rispettare le condizioni per ricorrere a un altro responsabile del trattamento (art. 28 par. 2 e par. 4 Regolamento UE 2016/679).

Il responsabile del trattamento non ricorrerà a un altro responsabile senza previa autorizzazione scritta specifica del Titolare del trattamento. Il sub-responsabile sarà chiamato a sottoscrivere, nei confronti del responsabile del trattamento, un accordo che rispetti le misure tecniche e organizzative poste dal presente accordo.

REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

In qualità di responsabile del trattamento, per i suddetti trattamenti, RESPONSABILE ESTERNO si impegna a tenere e aggiornare i registri del trattamento di cui all'art. 30 Regolamento UE n. 679/2016 nella forma e con i contenuti indicati dalla disposizione citata.

DURATA

Il presente accordo ha la durata dell'accordo di base, a decorrere da 01/01/20xx.

Al momento della conclusione del presente accordo, il responsabile del trattamento si impegna, su scelta del titolare del trattamento, a cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.

LUOGO, 02/01/20xx

Firma del Titolare del Trattamento
ORDINE TERRITORIALE ABCDE

_____

Con la firma in calce a tale documento accetto la nomina a **Responsabile del Trattamento** per i trattamenti prima riportati insieme alle loro caratteristiche peculiari

Firma del Responsabile del Trattamento
RESPONSABILE ESTERNO

_____

Ove applicabile, il presente documento annulla e sostituisce ogni altro documento di nomina a Responsabile del Trattamento di **RESPONSABILE ESTERNO** , già esistente e sottoscritto

Firma del Titolare del Trattamento
ORDINE TERRITORIALE ABCDE

_____

Firma del Responsabile del Trattamento
RESPONSABILE ESTERNO

_____

ALLEGATO 4

Esempio di Registro dei Data Breach

ultimo aggiornamento: 21/11/2023

Registro delle violazioni (artt. 33 e 34 gdpr)

obiettivo: **il titolare del trattamento, a prescindere dalla notifica al Garante, deve documentare tutte le violazioni dei dati personali. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.**

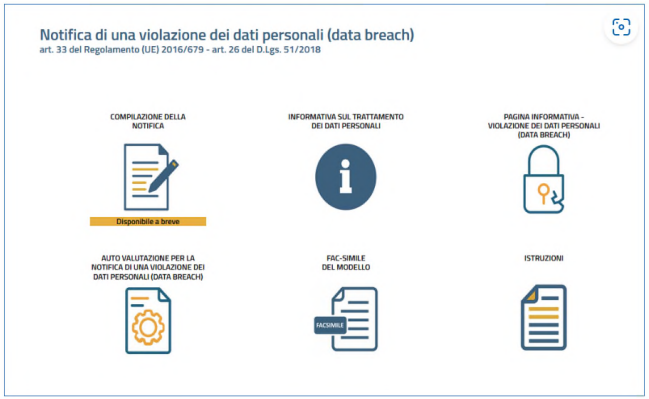
è opportuno anche documentare i "near miss", ovvero un evento che potenzialmente potrebbe causare un incidente

art, 34 comma 1

tipologia	evento	dettagli relativi alla violazione come tempi, modalità di esecuzione, data della scoperta;	cause che possono aver compromesso la situazione e portato al data breach;	fatti inerenti qualsiasi dettaglio che possa descrivere l'accaduto;	dati personali coinvolti e compromessi;	effetti della violazione;	Conseguenze della violazione;	provvedimenti adottati per rimediare all'accaduto;	ogni altro elemento necessario ad aggiungere dettagli che possano essere utili alla tutela degli interessati e al ripristino di condizioni di sicurezza.	è necessaria la comunicazione all'interessato?	è stata effettuata la segnalazione all'Autorità Garante?	se la risposta èSI, sono state rispettate le 72 ore dalla scoperta della violazione?	se la risposta è NO, indicare una breve nota illustrando la giustificazione della mancata denuncia di violazione
near miss													
data breach													

fonti di riferimento:

Linea guida		- Linee guida 9/2022 in materia di notifica delle violazioni di dati personali (data breach)
		- Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di violazione dei dati
GDPR		artt. 33 e seguenti
WP		Linee guida "WP250"
d.lgs. 51/2018		art. 26
testo		GDPR
codice privacy IT		Codice Privacy - Garante Privacy



ALLEGATO 5

Esempio di Registro dei Trattamenti

esempio di Registro dei trattamenti. I dati inseriti sono a titolo indicativo e non esaustivo

Di seguito è riportata la tabella di sintesi dei trattamenti eseguiti dal Titolare del trattamento: Ordine Medici Veterinari della Provincia di _____: ultimo aggiornamento: XXXX

	Trattamento	Finalità	basi giuridiche 1	basi giuridiche 2	Interessato	Trasferimento in paese extra UE	dati personali 1	dati personali 2	Periodo di conservazione	Misure di sicurezza
1	AZ02 - Acquisti *	Attività di acquisto di beni o servizi	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Fornitori	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Dati sul comportamento, profili di utenti, consumatori, contribuenti, ecc.	Banche e Istituti di credito. Autorità giudiziaria e/o autorità di pubblica sicurezza	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	Credenziali di autenticazione, accesso controllato, lettera di incarico al personale autorizzato, backup, regolamento aziendale sull'uso dei sistemi informatici, formazione ed istruzione al peronale autorizzato, etc
2	AZ15 - Smaltimento-Distruzione Documenti	Adempimenti in materia di protezione dei dati personali	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Clienti o Utenti; Personale dipendente; Fornitori; Consulenti e liberi professionisti, anche in forma associata	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Attività economiche, commerciali, finanziarie, assicurative	società di smaltimento pubblici uffici	Un mese	
3	COM001 - Prevenzione corruzione_trasparenza amm.va	Adempimenti in materia di Anticorruzione (Legge 6 novembre 2012, n. 190); Adempimenti in materia di Trasparenza (Decreto legislativo 14 marzo 2013, n. 33 (Amministrazioni comunali))	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Personale dipendente; Personale pubblico dirigenziale; Soggetti eletti; Iscritti all'Ordine Medici Veterinari	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Beni, proprietà, possesso; Dati di contatto (numero di telefono, e-mail, ecc.); Dati relativi alla situazione reddituale	Autorità giudiziaria e/o autorità di pubblica sicurezza	10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni); I dati sono mantenuti per sempre secondo le disposizioni vigenti	
4	COM002 - Procedure elettorali	Servizi demografici / Elettorale - Attività relativa all'elettorato attivo e passivo; Servizi demografici / Elettorale - Attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	Soggetti eletti; Iscritti all'Ordine Medici Veterinari; Componenti seggio elettorale	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale	Associazioni di categorie	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	

	Trattamento	Finalità	basi giuridiche 1	basi giuridiche 2	Interessato	Trasferimento in paese extra UE	dati personali 1	dati personali 2	Periodo di conservazione	Misure di sicurezza
5	COM005 - Procedure affid_ lavori_ servizi_forniture	Individuazione del miglior contraente	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Consulenti e liberi professionisti, anche in forma associata; Soggetti partecipanti a gare pubbliche	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Istruzione e cultura; Attività economiche, commerciali, finanziarie e assicurative; Certificati di qualità professionali; Certificati di qualità prodotti; Professione dichiarata; Dati di contatto (numero di telefono, e-mail, ecc.)	Banche e Istituti di credito. Autorità giudiziaria e/o autorità di pubblica sicurezza	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
6	COM103 - Procedimenti disciplinari	Gestione del contenzioso	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Iscritti all'Ordine Medici Veterinari	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Dati di contatto (numero di telefono, e-mail, ecc.); Dati inerenti situazioni giudiziarie civili, amministrative, tributarie,penale	Consulenti e liberi professionisti in forma singola o associata	10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
7	COM107 - Procedure gestione Accessi Documentali	Accesso agli Atti (Decreto del Presidente della Repubblica 12 aprile 2006, n. 184)	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Cittadini; Iscritti all'Ordine Medici Veterinari	No	Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Dati presenti in archivio		5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
8	COM112 - Segnalazione rappresentanti Ordine	Esecuzione di un compito di pubblico interesse (Decreto Legislativo 18 agosto 2000, n. 267)			Soggetti interessati all'attività istituzionale dell'Ordine	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Lavoro (occupazione attuale, precedente, curriculum, ecc.); Istruzione e cultura; Professione dichiarata; Dati di contatto (numero di telefono, e-mail, ecc.)		5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
9	Contabilità *	Gestione contabile o di tesoreria; Adempimenti fiscali	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Consulenti e liberi professionisti, anche in forma associata; Fornitori	No	Attività economiche, commerciali, finanziarie e assicurative; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Coordinate bancarie	; Consulenti e liberi professionisti in forma singola o associata	10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	

	Trattamento	Finalità	basi giuridiche 1	basi giuridiche 2	Interessato	Trasferimento in paese extra UE	dati personali 1	dati personali 2	Periodo di conservazione	Misure di sicurezza
10	GE03 - Gestione Fornitori *	Gestione dei fornitori	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Fornitori	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Coordinate bancarie; codice fiscale legale rappresentante società fornitrice, poteri di rappresentanza all'interno della società fornitrice, numero di telefono ed e-mail aziendale, numero di telefono ed e-mail aziendale dipendenti società fornitrice	; Consulenti e liberi professionisti in forma singola o associata	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
11	GE13 - Gestione Fatturazione Elettronica *	Adempimento di obblighi fiscali e contabili (Decreto legislativo del 05/08/2015 n. 127)	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Clienti o Utenti	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Natura dei beni; Provincia di residenza; Dati di contatto (numero di telefono, e-mail, ecc.)	Enti pubblici, clienti , banche e istituti di credito	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
12	GE35 - Assicurazioni Rischi dell'Ordine	Servizi assicurativi	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Soggetti eletti	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Attività economiche, commerciali, finanziarie e assicurative; Beni, proprietà, possesso; Immagini; Valore dei beni; Natura dei Servizi Professionali erogati	Enti pubblici. Compagnie di assicurazioni in caso di sinistri. Autorità Giudiziaria. Autorità di Pubblica Sicurezza	10 anni a decorrere dalla data di cessazione dei contratti con fornitori (art. 2220 codice civile che prevede la conservazione per 10 anni delle scritture contabili; art. 22 del D.P.R. 29 Settembre 1973, n.600)	
13	GE52 - Gestione Iscritti	Cura dei rapporti con gli assistiti	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Ente di Previdenza ENPAV; Federazione Nazionale FNOVI; Iscritti all'Ordine Medici Veterinari	No	Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Deposito firma su registro consegna timbro professionale tondo; Stato di salute	Associazione di categoria, Enti pubblici. Autorità Sanitaria. Compagnie di assicurazioni in caso di sinistri.	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni); I dati fanno parte dell'archivio storico dell'Ordine. I datii sono conservati in un apposito contenitore e rimangono a disposizione dell'Ordine per verifiche per tutta la durata della permanenza dell'associato nell'Ordine. L'Ordine tiene uno storico di tutti gi Albi annuali a tempo indeterminato in	

	Trattamento	Finalità	basi giuridiche 1	basi giuridiche 2	Interessato	Trasferimento in paese extra UE	dati personali 1	dati personali 2	Periodo di conservazione	Misure di sicurezza
14	GE53 - Gestione Consiglieri_Revisori Ordine	Servizi di controllo interno	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Soci, associati ed iscritti		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Coordinate bancarie; Provincia di residenza; Sesso m/f; Ruolo ricoperto in azienda; Dati di contatto (numero di telefono, e-mail, ecc.)	associazione di categoria	5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
15	YY22 -Gestione del Protocollo Informatico dell'Ordine	Gestione della corrispondenza in entrata ed in uscita	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Consulenti e liberi professionisti, anche in forma associata; Iscritti all'Ordine Medici Veterinari; Clienti o Utenti; Iscritti o potenziali iscritti; Personale dipendente; Lavoratori autonomi; Soggetti interessati all'attività istituzionale		Nominativo, indirizzo o altri elementi di identificazione personale; Indirizzo e-mail		5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
16	PR02 - Consulenza Legale	Consulenza legale	Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi		Clienti o Utenti; Consulenti e liberi professionisti, anche in forma associata; Fornitori; Lavoratori autonomi; Agenti e rappresentanti		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Attività economiche, commerciali, finanziarie e assicurative; Beni, proprietà, possesso	Enti pubblici. Compagnie di assicurazioni in caso di sinistri. Autorità Giudiziaria. Autorità di Pubblica Sicurezza	10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
17	PR06 - Consulenza Tributaria *	Adempimento di obblighi fiscali e contabili			Clienti o Utenti; Personale dipendente; Fornitori; Stagisti; Lavoratori somministrati		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Attività economiche, commerciali, finanziarie e assicurative		10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
18	TC25 - Realizzazione del tesserino professionale	Attività promozionali	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Iscritti all'Ordine Medici Veterinari		Nominativo, indirizzo o altri elementi di identificazione personale; Codice fiscale ed altri numeri di identificazione personale		10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	

	Trattamento	Finalità	basi giuridiche 1	basi giuridiche 2	Interessato	Trasferimento in paese extra UE	dati personali 1	dati personali 2	Periodo di conservazione	Misure di sicurezza
19	SP08 - Reception	Controllo degli accessi fisici e monitoraggio delle persone che fanno ingresso in azienda; Filtraggio delle telefonate	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi	Clienti o Utenti; Consulenti e liberi professionisti, anche in forma associata; Fornitori; Iscritti all'Ordine Medici Veterinari; Personale dipendente		Dati di contatto (numero di telefono, e-mail, ecc.); Nominativo, indirizzo o altri elementi di identificazione personale; Professione dichiarata		Tre mesi	
20		Monitoraggio delle persone che fanno ingresso in azienda); Filtraggio delle telefonate	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi	Clienti o Utenti; Consulenti e liberi professionisti, anche in forma associata; Iscritti all'Ordine Medici Veterinari; Fornitori; Personale dipendente; Cittadini		Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Professione dichiarata		Tre mesi	
21	SA55 - Assistenza Sociale	Attività di assistenza sociale a favore degli assistiti; Cura dei rapporti con gli assistiti; Cura dei rapporti con i familiari degli assistiti	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Familiari degli assistiti; Soci, associati ed iscritti		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati relativi alla famiglia o a situazioni personali; Dati di contatto (numero di telefono, e-mail, ecc.); Dati relativi alla situazione reddituale; Stato di salute		5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
22		Attività di assistenza sociale a favore degli assistiti; Cura dei rapporti con gli assistiti; Cura dei rapporti con i familiari degli assistiti	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Familiari degli assistiti; Soci, associati ed iscritti		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Dati relativi alla famiglia o a situazioni personali; Dati di contatto (numero di telefono, e-mail, ecc.); Dati relativi alla situazione reddituale; Stato di salute		5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	

	Trattamento	Finalità	basi giuridiche 1	basi giuridiche 2	Interessato	Trasferimento in paese extra UE	dati personali 1	dati personali 2	Periodo di conservazione	Misure di sicurezza
23	SC51 - Tenuta Albo Professionale	Gestione Albo Professionale (*_Obblighi legale al quale è soggetto il titolare del trattamento)	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Soci, associati ed iscritti		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Istruzione e cultura; Dati inerenti situazioni giudiziarie civili, amministrative, tributarie,penale		10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
24	SC71 - Gestione Formazione Online	Formazione e informazione professionale degli iscritti e partecipazione ad eventi istituzionali	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Soci, associati ed iscritti		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Provincia di residenza; Cookie tecnici; Dati di contatto (numero di telefono, e-mail, ecc.); Videoregistrazioni	Associazione di categoria, Enti di formazione, banche e istituti di credito	10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
25	SP04 - Formazione Privacy	Adempimenti in materia di protezione dei dati personali	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Soci, associati ed iscritti; Stagisti; Personale dipendente		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Ruolo ricoperto in azienda	Associazione di categoria, Enti di formazione, banche e istituti di credito	10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
26	SP05 - Formazione	Formazione del personale	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Soci, associati ed iscritti		Ruolo ricoperto in azienda; Nominativo, indirizzo o altri elementi di identificazione personale; Idoneità al lavoro; Certificati di qualità professionali	Associazione di categoria, Enti di formazione, banche e istituti di credito	10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	
27	SP44 - Anagrafe Tributaria *	Adempimenti fiscali	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Soci, associati ed iscritti		Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale		5 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	

	Trattamento	Finalità	basi giuridiche 1	basi giuridiche 2	Interessato	Trasferimento in paese extra UE	dati personali 1	dati personali 2	Periodo di conservazione	Misure di sicurezza
28	TC01 - Gestione sito Web *	Informazione per via telematica	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Iscritti all'Ordine Medici Veterinari; Clienti o Utenti		Nominativo, indirizzo o altri elementi di identificazione personale; Provincia di residenza; Dati di contatto (numero di telefono, e-mail, ecc.)	Società di assistenza IT/Web master	I dati fanno parte dell'archivio storico dell'Ordine. I datii sono conservati in un apposito contenitore e rimangono a disposizione dell'Ordine per verifiche per tutta la durata della permanenza dell'associato nell'Ordine. L'Ordine tiene uno storico di tutti gi Albi annuali a tempo indeterminato in apposito armadio chiuso a chiave	
29	TC02 - Manutenzione Software di Base *	Assistenza utenti	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Clienti o Utenti; Fornitori		Nominativo, indirizzo o altri elementi di identificazione personale; Codice fiscale ed altri numeri di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Natura dei beni; Valore dei beni; Certificati di qualità professionali	Società di assistenza IT/Web master	10 anni a decorrere dalla data di cessazione dei contratti con fornitori (art. 2220 codice civile che prevede la conservazione per 10 anni delle scritture contabili; art. 22 del D.P.R. 29 Settembre 1973, n.600)	
30	TC12 - Manutenzione Hardware *	Assistenza utenti	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Clienti o Utenti; Fornitori		Nominativo, indirizzo o altri elementi di identificazione personale; Codice fiscale ed altri numeri di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Natura dei beni; Valore dei beni; Certificati di qualità professionali	Società di assistenza IT/Web master	10 anni a decorrere dalla data di cessazione dei contratti con fornitori (art. 2220 codice civile che prevede la conservazione per 10 anni delle scritture contabili; art. 22 del D.P.R. 29 Settembre 1973, n.600)	
31	TC26 - Timbri Iscritti	Attività promozionali	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Soci, associati ed iscritti		Nominativo, indirizzo o altri elementi di identificazione personale		10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	

	Trattamento	Finalità	basi giuridiche 1	basi giuridiche 2	Interessato	Trasferimento in paese extra UE	dati personali 1	dati personali 2	Periodo di conservazione	Misure di sicurezza
32	VE01- Appelli Smarrimenti - Bacheca *	Assistenza utenti	L'interessato deve esprimere il consenso al trattamento dei propri dati personali per la specifica finalità		Clienti o Utenti		Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Argomenti di interesse; Stato di salute attuale o pregresso dell'animale	canili,	I dati fanno parte dell'archivio storico dell'Ordine. I datii sono conservati in un apposito contenitore e rimangono a disposizione dell'Ordine per verifiche per tutta la durata della permanenza dell'associato nell'Ordine. L'Ordine tiene uno storico di tutti gi Albi annuali a tempo indeterminato in apposito armadio chiuso a chiave	
33	YY02 - Gestione Corrispondenza	Gestione della clientela; Gestione del personale ; Adempimenti in materia di protezione dei dati personali	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Clienti o Utenti; Potenziali clienti; Personale dipendente; Consulenti e liberi		Nominativo, indirizzo o altri elementi di identificazione personale; Indirizzo e-mail		10 anni a decorrere dalla data di cessazione dei contratti con fornitori (art. 2220 codice civile che prevede la conservazione per 10 anni	
34	YY05 - Gestione delle Telefonate	Assistenza utenti	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Clienti o Utenti		Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Argomenti di interesse		Tre mesi	
35	YY10 - Gestione delle Chiavi e Password	Gestione del patrimonio mobiliare e immobiliare ; Servizi di controllo interno ; Adempimenti in materia di protezione dei dati personali	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento		Clienti o Utenti; Potenziali clienti; Personale dipendente; Consulenti e liberi professionisti, anche in forma associata; Stagisti; Visitatori sito web		Nominativo, indirizzo o altri elementi di identificazione personale; Dati di contatto (numero di telefono, e-mail, ecc.); Indirizzo e-mail; Attività economiche, commerciali, finanziarie, assicurative; Dati inerenti situazioni giudiziarie civili, amministrative, tributarie,penale		10 anni a decorrere dalla data di cessazione dei contratti con fornitori (art. 2220 codice civile che prevede la conservazione per 10 anni delle scritture contabili; art. 22 del D.P.R. 29 Settembre 1973, n.600)	
36	YY33 - Creazione e gestione caselle PEC degli Iscritti	Servizi di intermediazione	Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso		Soci, associati ed iscritti		Nominativo, indirizzo o altri elementi di identificazione personale; Indirizzo e-mail; Codice fiscale ed altri numeri di identificazione personale; Provincia di residenza; Dati di contatto (numero di telefono, e-mail, ecc.)		10 anni a decorrere dalla data di cessazione del contratto (art. 2948 codice civile che prevede la prescrizione di 5 anni)	

CONTATTI

Ordine Capofila per la realizzazione dei Codici di Condotta:

ORDINE DEI MEDICI VETERINARI DELLA PROVINCIA DI VARESE
INDIRIZZO Via dei Campigli, 5 - 21100 VARESE (VA)
TELEFONO 0332/285679
FAX 0332/311857
E-MAIL segreteria@ordineveterinari.va.it
PEC ordinevet.va@pec.fnovi.it