

# Innovando GmbH

Dorfstrasse, 29

9108 Gonten

Tel: +41717941500

P.IVA CHE396.086.464

## Il Titolare

**Titolare : Innovando GmbH nella persona di Andreas Voigt**

**La Legge definisce come titolare la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.**

Al titolare spettano, per presunzione assoluta di legge, la direzione delle attività di trattamento dei dati personali: a tale soggetto competono infatti le decisioni strategiche di fondo su come (modalità) e perché (finalità) raccogliere e trattare i dati, nonché sull'organizzazione del trattamento e sulle risorse (strumenti) da dedicarvi, anche per garantire la sicurezza. Il titolare si identifica con la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo cui oggettivamente spettano tali decisioni di fondo.

Nel caso di persone giuridiche, tale figura tende in generale a coincidere con il legale rappresentante della società o dell'ente potendosi così individuare, anche nell'ambito di strutture complesse, chi sia specificamente: tale soggetto sarà sempre e comunque tenuto in prima persona a rispondere per i danni cagionati nel trattamento dei dati, nonché delle sanzioni di carattere civilistico ed amministrativo.

E' inoltre possibile che, da parte delle autorità preposte all'accertamento degli eventuali reati, le responsabilità di ordine penale vengano estese a tutti i componenti dell'organo cui spetta la direzione della società e dell'ente (ad esempio, i membri del Consiglio di Amministrazione).

## Compiti del Titolare

E' compito del titolare:

- Mettere in atto e verificare l'applicazione di tutte le disposizioni di legge in ordine ai trattamenti di dati personali in corso.
- Adottare e verificare l'implementazione delle misure di sicurezza previste dal Codice della Privacy per garantire l'idonea protezione ai dati, ponendo particolare attenzione alle misure minime di sicurezza.
- Individuare e nominare gli incaricati ai trattamenti di dati personali, per iscritto e fornendo loro istruzioni per poter operare in modo corretto e secondo quanto disposto dal Codice della Privacy anche in riferimento alle misure di sicurezza.
- Eventualmente individuare e nominare dei responsabili tramite lettera di nomina scritta definendo le aree di competenza (trattamento dei dati, sicurezza, gestione dei sistemi di elaborazione elettronica, rapporto con gli interessati) e i compiti assegnati.
- Provvedere a fornire a Responsabili e Incaricati l'adeguata istruzione riguardo le disposizioni di legge contenute nel Codice della Privacy che regolano le responsabilità, le funzioni e gli scopi propri della loro mansione nonché le norme basilari relative ai trattamenti e alla protezione dei dati.
- Il Titolare del trattamento può ritenere di non nominare alcun responsabile con la consapevolezza di accollarsi per intero le responsabilità e le funzioni loro proprie. In questo caso sarà sua preoccupazione realizzare l'intero adeguamento di Legge secondo tutte le norme e le disposizioni in essa contenute.

**In particolare, non essendo stati nominati dei Responsabili in tutte le aree di competenza, sono sotto riportati, divisi per aree di competenza, i compiti che devono essere eseguiti dal titolare, almeno fino alla nomina dei relativi Responsabili.**

## Trattamento dei dati

L'area 'trattamento dati' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni inerenti alla gestione dei rapporti tra il Titolare e il Garante, tra il Titolare e gli interessati, e alla gestione operativa dei trattamenti dei dati personali:

- gestione notifica
- gestione rapporti con il Garante
- verifica corrispondenza con Autorizzazioni Annuali
- gestione comunicazione e diffusione dei dati secondo legge
- gestione informativa e consenso verso interessati
- gestione diritti di accesso degli interessati
- gestione delle modalità dei trattamenti interni
- nomina degli incaricati del trattamento
- creazione e gestione dei profili di autorizzazione
- gestione dei trattamenti affidati a terzi
- gestione della formazione da impartire agli incaricati

Individuare e nominare Incaricati dei trattamenti tutti coloro che sono addetti al trattamento esecutivo dei dati personali.

È compito del Responsabile ai Trattamenti:

- Raggiungere un sufficiente grado di apprendimento in materia di Privacy in modo da poter trattare i dati secondo la Legge e realmente vigilare sulla liceità e sulla correttezza dei trattamenti.
- Predisporre la notificazione iniziale al Garante nel caso in cui il trattamento rientri nei casi contemplati dall'art.37 del Codice, attraverso il programma Web disponibile sul sito del Garante ([www.garanteprivacy.it](http://www.garanteprivacy.it)), verificando l'esattezza e la completezza dei dati contenuti.
- Interagire con il Garante, in caso di richieste di informazioni o effettuazione di controlli ed accessi da parte dell'autorità;
- Censire analiticamente le banche dati con tutti gli elementi necessari per la determinazione dei trattamenti e delle tipologie di dati da inserire nel MANUALE ORGANIZZATIVO DELLA PRIVACY (dati trattati, tipi di trattamento, categorie di interessati, sedi e uffici del trattamento e in collaborazione con il Responsabile della Sicurezza, l'elenco dei sistemi di elaborazione nei quali avvengono i trattamenti), anche ai fini della eventuale notifica al Garante;
- Verificare che i trattamenti dei dati sensibili rientrino nelle Autorizzazioni del Garante in corso di validità ed, eventualmente, predisporre la richiesta di autorizzazione preventiva al trattamento di dati sensibili nel caso in cui il trattamento non rientri in tali Autorizzazioni.
- Procedere alla gestione delle informative e delle richieste di consenso nei casi e nelle modalità previste dalla legge
- Gestire il diritto di accesso degli interessati, agendo prontamente per soddisfare le loro richieste secondo l'art. 7; a questo proposito il Responsabile del trattamento ha la facoltà di nominare un Responsabile del Diritto di Accesso, al quale può delegare tale compito.
- Aggiornare l'elenco dei trattamenti in relazione ad eventuali nuovi trattamenti di dati personali;
- Individuare e nominare gli incaricati del trattamento impartendo loro, per iscritto, la nomina, le istruzioni e le autorizzazioni necessarie ad un corretto, lecito e sicuro trattamento, verificandone la puntuale applicazione;
- Produrre le nomine, le istruzioni e la distribuzione dei compiti (mansionario privacy) da consegnare ai medesimi per la firma e l'archiviazione.
- Collaborare con eventuali altri Responsabili e con l'eventuale Amministratore di Sistema.
- Definire i profili di autorizzazione (ambiti di competenza e operazioni consentite) degli incaricati
- Autorizzare i singoli incaricati al trattamento specifico di dati sensibili e giudiziari ponendo bene in evidenza tale fatto nella definizione del profilo di autorizzazione;
- Tenere aggiornato l'elenco dei trattamenti (censimento delle banche dati, tipologie di dati trattati, sedi in cui vengono trattati) e la distribuzione dei compiti (mansionario della privacy), con cadenza almeno annuale.
- Periodicamente con cadenza almeno annuale verificare la correttezza dei profili di autorizzazione revisionando gli ambiti di competenza ed eventualmente adattandoli a nuove esigenze.
- Provvedere a eliminare le autorizzazioni che rimangono inutilizzate oltre i sei mesi, sempre che il profilo particolare non determini per propria definizione un trattamento sporadico.
- Attuare gli obblighi di informazione ad acquisizione del consenso, quando richiesto, nei confronti degli interessati; delegare eventualmente questa incombenza ai singoli incaricati. A tal fine è possibile utilizzare i moduli e le procedure predisposte attraverso il Portale della Privacy.
- Individuare i trattamenti che vengono ceduti a Terzi (ad es. la gestione delle paghe) e attuare i necessari provvedimenti affinché tali trattamenti avvengano secondo liceità e correttezza garantendo lo standard di sicurezza previsto dalla legge. Il Responsabile deve decidere se nominare Responsabile la società terza in oggetto, se nominare Incaricati i soggetti individuali terzi che materialmente effettueranno i trattamenti o se introdurre restrittive clausole di garanzia nel contratto di fornitura del servizio. In queste operazioni può collaborare con l'eventuale Responsabile dell'area sicurezza.
- Verificare che tutti i trattamenti avvengano nel rispetto delle disposizioni di legge.
- Distruggere i dati personali che non sono più oggetto di trattamento alcuno.
- Informare prontamente il Titolare ed il personale interno addetto alla privacy di ogni questione rilevante ai fini di legge;
- Comunicare al Titolare qualsiasi elemento oggettivo o soggettivo che possa compromettere il corretto trattamento dei dati personali.
- Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del Titolare; nel caso venga delegato il trattamento all'esterno gestire il trattamento tramite terzi attuando le misure necessarie affinché sia garantita la sicurezza dei dati esportati, questo anche in collaborazione con l'eventuale Responsabile dell'area sicurezza.
- Collaborare con l'eventuale Responsabile dell'area sicurezza e con l'eventuale Amministratore di Sistema nella definizione delle credenziali di autenticazione e dei profili di autorizzazione.
- Elaborare un piano di formazione per rendere edotti gli incaricati del trattamento delle disposizioni di legge sulle modalità e i criteri del trattamento, nonché dei rischi individuati e dei modi per prevenire danni, anche in collaborazione con gli altri Responsabili.
- Collaborare con tutti i responsabili per l'attuazione delle prescrizioni impartite dal Garante attraverso nuove circolari, autorizzazioni e aggiornamenti di Legge;
- Nel caso di Aziende sanitarie gestire la cifratura e la separazione nei casi in cui vi sia la coesistenza di dati identificativi dell'interessato e dati sensibili, con particolare riferimento a quelli sanitari, che consentano una immediata associazione tra di essi.

## Sicurezza

L'area 'sicurezza' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni inerenti alla implementazione delle misure di sicurezza atte a proteggere in modo preventivo e idoneo (art. 31 del Codice) i dati personali oggetto di trattamento e, in particolare, delle Misure Minime di Sicurezza trattate dagli artt. 33, 34, 35, 36 e dall'Allegato Disciplinare Tecnico B, ponendo estrema attenzione ai trattamenti di dati sensibili e giudiziari:

E' compito del Responsabile individuare e nominare, se lo ritiene opportuno, un Amministratore di Sistema ed eventualmente un incaricato alla custodia delle copie credenziali. E' altresì suo compito nominare eventualmente un incaricato al controllo degli accessi ai locali e obbligatoriamente un incaricato alla sorveglianza dell'archivio ad accesso autorizzato se dovessero esistere all'interno della struttura del Titolare archivi cartacei o contenitori di supporti informatici rimuovibili, contenenti dati sensibili o giudiziari.

Se il Responsabile della sicurezza decidesse di non nominare nessun amministratore di sistema od incaricato, se ne assumerà interamente le funzioni, i compiti e le responsabilità in relazione alla sicurezza dei dati personali.

È compito del Responsabile della Sicurezza:

- Se il trattamento dei dati personali è effettuato con l'ausilio di strumenti informatici, censire tutti i sistemi di elaborazione elettronica indicandone le caratteristiche principali (sistemi operativi, gestione multiprofilo, programmi di protezione, sistemi di antintrusione, programmi di elaborazione dei dati) e aggiornare, con cadenza annuale, l'elenco di tali sistemi.
- Individuare la dislocazione fisica dei trattamenti e in particolare:
- le aree e i locali nei quali si trovano gli elaboratori o i sistemi di accesso remoto alle banche dati elettroniche e in particolare i sistemi che consentono l'accesso a dati sensibili o giudiziari; per tali aree e locali è bene nominare un incaricato al controllo accessi.
- gli uffici e gli archivi nei quali vengono trattati e riposti dati sensibili o giudiziari; per tali archivi è necessario nominare un incaricato alla sorveglianza.
- Definire e verificare le modalità di accesso a tali locali e le misure da adottare per la protezione dei medesimi;
- predisponendo i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati nonché le procedure per controllare l'accesso delle persone autorizzate;
- impartendo specifiche istruzioni agli incaricati al controllo e alla sorveglianza delle aree e dei locali nonché degli archivi contenenti dati sensibili o giudiziari.
- Rendere esecutive tutte le misure di sicurezza adottate per la protezione dei dati personali e verificare la loro corretta implementazione con cadenza, almeno, semestrale.
- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate anche all'esterno nel caso venga affidato a terzi il trattamento dei propri dati personali; collaborare in tal senso con il Responsabile all'area 'trattamento dati' che ha compiti specifici.
- Definire i criteri e le procedure per la sicurezza delle trasmissioni dei dati siano esse fatte attraverso fax o posta elettronica, ivi compresi quelli per le restrizioni di accesso per via telematica;
- Definire la politica di accesso alla rete da parte dei dipendenti, le loro responsabilità e le restrizioni in ordine alla sicurezza. Raccogliere, eventualmente, presso i dipendenti una assunzione di responsabilità per i siti visitati, nel caso venga loro concesso di navigare per proprio ed esclusivo interesse durante l'orario di lavoro.
- Relativamente alle disposizioni del punto precedente, è opportuno definire le modalità di gestione dei files di LOG da parte della direzione, fornendo a tal proposito espressa informativa e richiesta di consenso al trattamento dei medesimi: è da considerare il fatto che nei file di log siano contenuti dati personali anche sensibili. La direzione deve tenere in considerazione che il controllo dei log files rientra nelle disposizioni contenute nello Statuto dei Lavoratori art. 4 (Sorveglianza sul posto di lavoro).
- Custodire i supporti informatici adibiti alle copie di sicurezza dei dati impartendo istruzioni all'Amministratore di Sistema o all'incaricato della gestione e della manutenzione del sistema.
- Pianificare ed eseguire di test del sistema di sicurezza, attraverso adeguate prove di penetrazione
- Definire ed attuare di piani e strumenti di monitoraggio continuo della sicurezza
- Aggiornare periodicamente il sistema di sicurezza, per renderlo sempre adeguato alle nuove minacce
- Manutenere il sistema di sicurezza, per assicurarne costante efficienza e disponibilità
- Fornire supporto alla formazione del personale dell'organizzazione, in tema di sicurezza
- Emanare procedure interne inerenti la sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, ecc).
- Distruggere in modo definitivo i supporti rimuovibili informatici destinati ad essere cestinati con particolare attenzione a quelli che contenevano dati personali sensibili;
- Distruggere le memorie fisse (Hard Disk) dei PC che eventualmente vanno in rottamazione.

## Gestione dei sistemi di elaborazione elettronica.

L'area 'sistemi di elaborazione elettronica' comprende l'espletamento di tutte le operazioni inerenti alla gestione e alla manutenzione del sistema informatico non solo in rapporto alle soluzioni tecnologiche ma anche in ordine alle disposizioni di Legge in materia di sicurezza dei dati.

È compito del Responsabile individuare e nominare, se lo ritiene opportuno, uno o più incaricati alla manutenzione del sistema. Deve collaborare con gli altri responsabili nell'individuare e nominare gli incaricati al Back-up dei dati personali.

Se il Responsabile decidesse di non nominare nessun incaricato se ne assumerà le funzioni, i compiti e le responsabilità interamente.

È compito del Responsabile:

- Se il trattamento avviene con l'ausilio di mezzi informatici, deve redigere e aggiornare l'elenco dei sistemi hardware e software interessati al trattamento dei dati personali
- Attivare e gestire le credenziali di autenticazione degli incaricati ai trattamenti collaborando col Responsabile all'area 'trattamento dati' e col Responsabile alla sicurezza.
- Istruire gli incaricati dei trattamenti sull'uso delle parole chiave e sulle modalità per la loro modifica in autonomia, facendo riferimento alle relative istruzioni degli incaricati al trattamento.
- Revocare e disattivare le credenziali di autenticazione agli incaricati che per qualunque motivo perdano la loro qualifica di incaricato
- Collaborare con il responsabile del trattamento nella definizione dei profili di autorizzazione definendo i trattamenti consentiti.
- Definire le politiche di protezione dei sistemi verso l'attacco di programmi (Virus) per tutte le basi dati elettroniche;
- Istruire l'incaricato alla manutenzione del sistema affinché le operazioni di riparazione e ripristino avvengano nel rispetto delle disposizioni di legge: in particolare dovrà attivare le necessarie azioni previste in caso gli elaboratori vengano spediti verso altra struttura per essere sottoposti alle necessarie riparazioni (vedi Trattamento terzi, clausole contrattuali) anche in collaborazione con il Responsabile dei trattamenti.
- La nomina a Responsabile Amministratore di Sistema può essere revocata in qualsiasi momento dal Titolare senza preavviso ed eventualmente affidata ad altro soggetto.

## Rapporto con gli Interessati

L'area 'rapporto con gli interessati' comprende l'espletamento degli obblighi di legge e l'esecuzione di tutte le operazioni volte a soddisfare i diritti sanciti dall'art.7 del Codice della privacy.

È compito del Responsabile:

- Conoscere i modi e i tempi entro i quali venire incontro alle richieste dell'interessato (artt.7, 8, 146).
- Prendere in carico tempestivamente e non oltre le 24 ore successive al loro ricevimento, i reclami degli interessati e le eventuali istanze del garante.
- Effettuare la ricerca dei dati richiesti, producendone una copia rispondente ai criteri di intelligibilità e chiarezza stabiliti dalla legge.
- Informare il titolare nel caso in cui dovessero intervenire delle difficoltà nella raccolta dei dati tali da compromettere in parte o del tutto la buona riuscita dell'operazione.