PRIVACY

o della

“protezione dei dati personali”

Privacy e Organizzazioni Religiose
www.studioprivacy.eu

PRESENTAZIONE

PARO ANDREA

- DPO e Consulente Privacy con più di 15 anni di esperienza specialistica Privacy
- Fondatore di Gemini Consult Srl e Studio Privacy
- Socio Fondatore Assoprivacy
- Associato Federprivacy
- Codice Nr. 2685 e Certificazione Liv. 5 Professional Partner ANIP
- Certificato TÜV Italia CDP_026

paro@geminiconsult.it - Mob. 348.7427151

PARO ANDREA, 50 anni sposato con 2 figlie. Da 30 anni si occupa di Sistemistica, Networking, Security IT e Consulenza in materia di sicurezza dei dati, con particolare riguardo alle tematiche Privacy.
I suoi studi sono di estrazione tecnico-economica ed è certificato TÜV "Privacy Officer", componente di Federprivacy e delegato Assoprivacy per il Veneto. E' iscritto all'ANIP (Albo Nazionale Informatici Professionisti con il nr. 2685) ed è Presidente del Collegio di Treviso. E' Titolare di Gemini Consult Srl, azienda nata nel 1997 e specializzata, oggi, in soluzioni di consulenza tecnico-legale sulla sicurezza e riservatezza delle informazioni. Inoltre è tra i fondatori di Studio Privacy, Privacy Consulting Group tra i più grandi d'Italia in termini di Clienti e Consulenze erogate.
Attualmente è DPO per diverse Aziende Private, anche internazionali, e Pubbliche. Insieme al suo Gruppo di Lavoro cura la Consulenza Privacy per diverse centinaia di aziende ed enti sia privati che pubblici, appartenenti ai settori merceologici e/o produttivi più disparati. E' specializzato nella progettazione, realizzazione e controllo di Sistemi di Gestione della raccolta e gestione delle informazioni e sul loro trattamento confidenziale e protezione. E' Docente in diversi corsi di formazione in materia di Privacy ed uso sicuro delle tecnologie digitali.

PRINCIPI GENERALI

QUADRO NORMATIVO

- Direttiva Europea 95/46/CE
- Legge 675 del 31 dicembre 1996
- D.Lgs 196 del 30 giugno 2003
- Provvedimenti diversi GdP
- Nuovo Regolamento Europeo GDPR 2016/679
- D.Lgs 101/18 e nuova 196/03

Trattato sul funzionamento dell'Unione europea (TFUE)

"Ogni Persona ha diritto alla protezione dei dati personali che la riguardano"

(Articolo 16, paragrafo 1)

D.Lgs 196/03

OGGETTO DELLA NORMATIVA

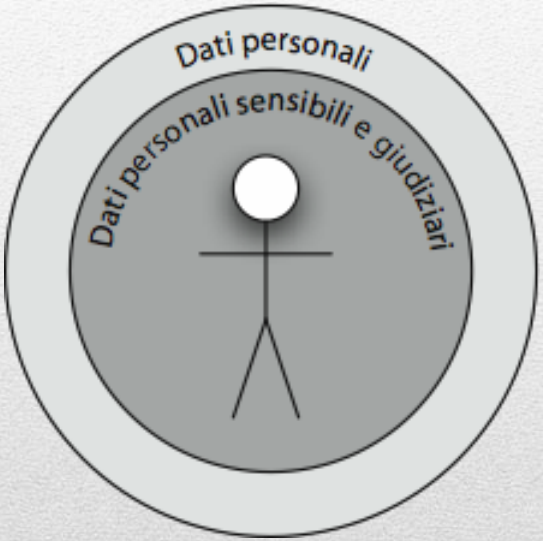
Il presente Codice **garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato**, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. (Art. 2. Finalità)

L'OFS e la Privacy

La situazione per l'OFS rispetto al trattamento dei dati dei Novizi, Professi e GIFRA, per le proprie Radici, per la propria storia e le proprie prassi pluri-secolari, non è di semplice definizione. **L'Ordine si basa sul concetto di semplicità, di umiltà e di rispetto introdotti e fortemente voluti da San Francesco.** Sostanzialmente l'adesione alla Regola più che un atto formale è innanzitutto **un'adesione radicale al Vangelo** il quale si fa Vita nella vita del francescano secondo uno stile di vita, una Regola, peculiari. Ovviamente **questa visione dell'appartenenza, plurisecolare, non prevede alcuna scheda di adesione**, né firme contrattuali (come ad es. per il matrimonio e/o il battesimo) ma solo una "spinta del cuore".

Così come, per contro, questo stile plurisecolare, **permeato dal rispetto e dall'attenzione particolare alla Persona**, ha sempre comportato **un sostanziale rispetto ed attenzione ai dati e alle informazioni relative ai confratelli e alle consorelle**. Sempre sostanzialmente attenti e discreti (almeno verso l'esterno) riguardo a situazioni personali e dati, registri e verbali di Fraternità. **Quasi avessimo ricevuto una particolare formazione Privacy che ci ha dato un particolare orientamento alla riservatezza** (e questo è per noi un enorme vantaggio rispetto ad altre Associazioni Ecclesiali).

I DATI



Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Identificativi: tutte le informazioni associabili direttamente o indirettamente ad un individuo;

Sensibili (Ultra Sensibili, Genetici e Biometrici): sottoinsieme dei dati personali, sono quelle informazioni riferibili al nucleo più intimo della persona;

Giudiziari: dati personali idonei a rivelare provvedimenti di ordine giudiziale;

Anonimi: dati che in origine o a seguito del trattamento non possono essere associati ad un interessato identificato o identificabile; quindi il dato può essere considerato anonimo quando è impossibile risalire all'interessato anche a seguito di trattamento.

Rif. art. 4 GDPR 2016/679 e art. 4 D.Lgs 196/03

TRATTAMENTO (GDPR Art. 4 p. 2)

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come:

Raccolta;
Registrazione;
Organizzazione;
Strutturazione;
Conservazione;
adattamento o modifica ;
Estrazione;
Consultazione;
Uso;

comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione;
Raffronto o Interconnessione;
Limitazione;
Cancellazione o la Distruzione

Diritto alla portabilità dei dati

Diritto alla «portabilità» dei propri dati personali per **trasferirli da un titolare del trattamento ad un altro** (ad es. cambio Social o provider di posta. Cambio ”lavoro”? Cambio “banca”? Cambio “Studio Legale”?)

Diritto all’oblio

Gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento **se**:

- i dati sono trattati solo sulla base del **consenso**;
- i dati **non sono più necessari** per gli scopi rispetto ai quali sono stati raccolti;
- i dati sono **trattati illecitamente**;
- l’interessato **si oppone legittimamente** al loro trattamento.

CESSAZIONE del TRATTAMENTO

Quando i Dati vengono:

1. **distrutti**
2. **ceduti** ad altro titolare – purche' destinati ad un trattamento compatibile agli scopi per i quali i dati sono stati raccolti;
3. conservati per **fini esclusivamente personali** (NO comunicazione/diffusione)
4. conservati/ceduti ad altro titolare per **scopi storici/statistici/scientifici**

LE FIGURE PRIVACY

LE FIGURE CHIAVE

DEL TRATTAMENTO

DI TUTELA

INTERESSATO

TITOLARE

Responsabile della protezione dei dati

Delegato al trattamento

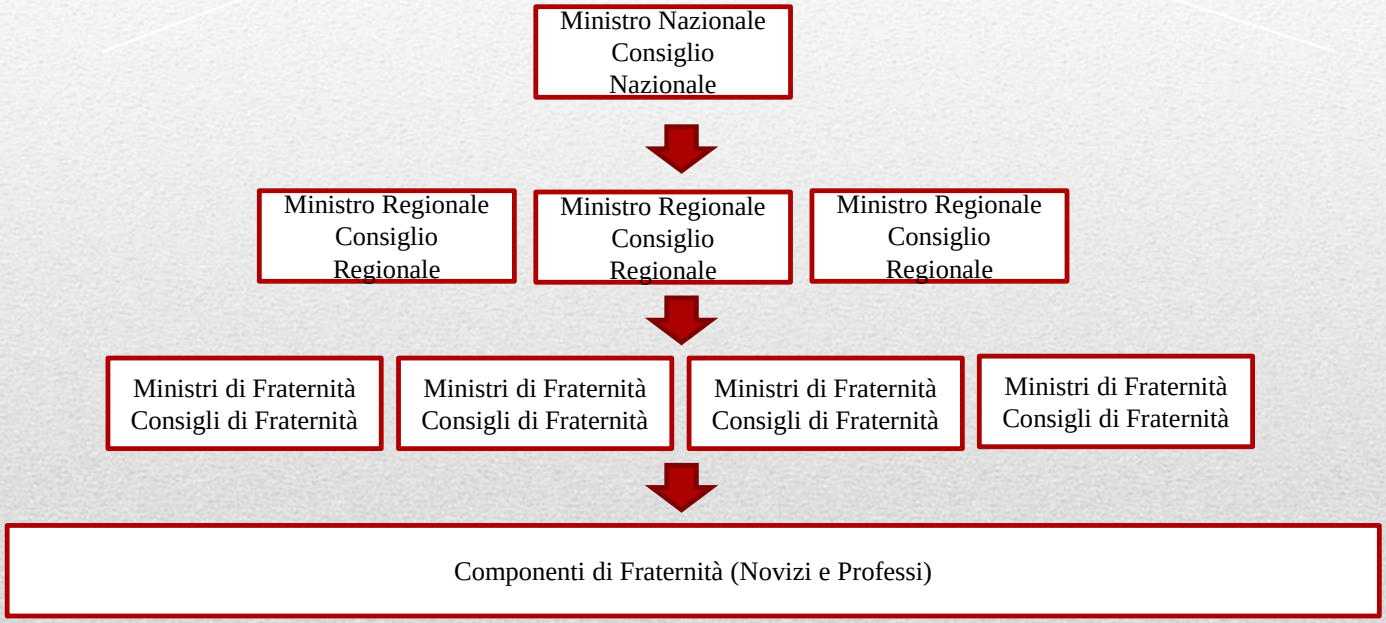
Incaricato

Amministratore di Sistema

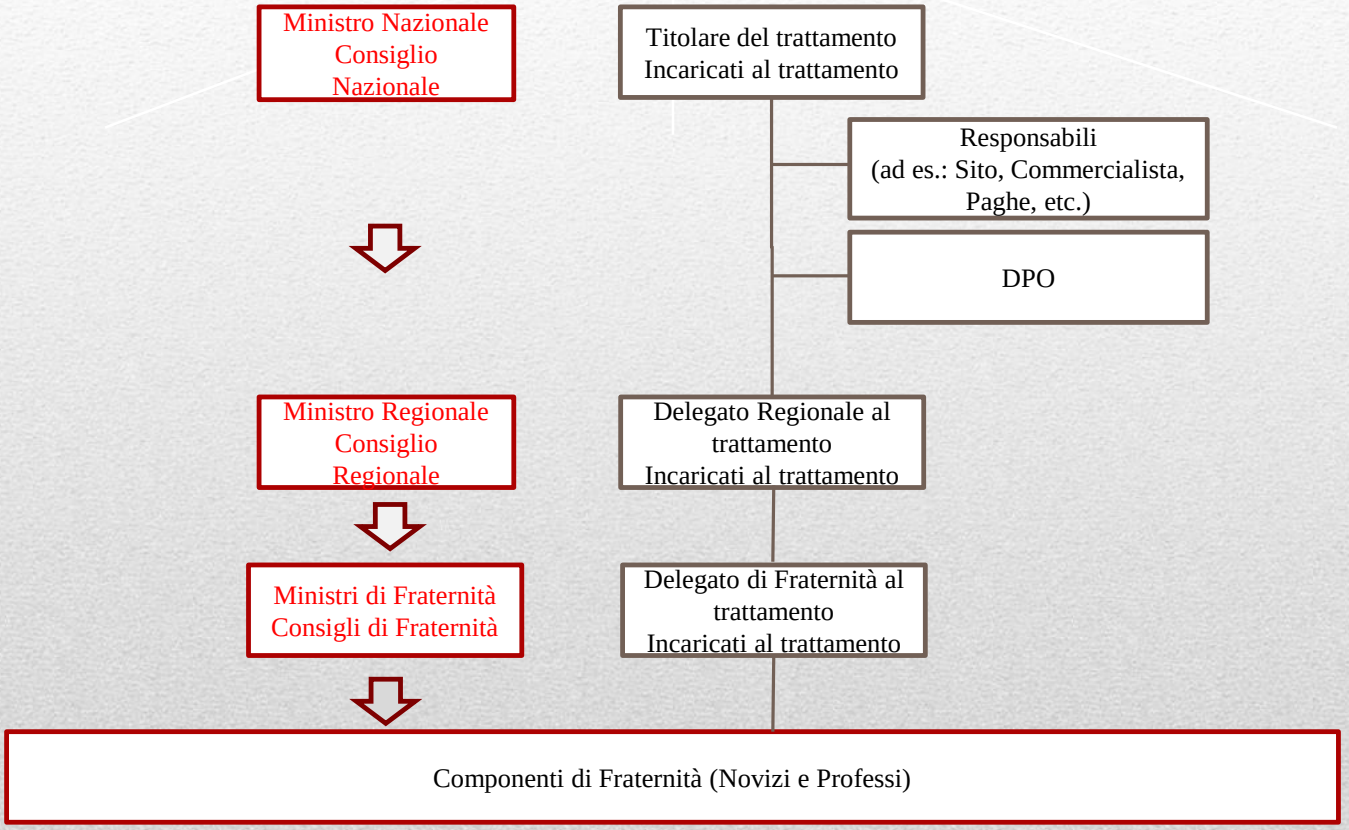
DI CONTROLLO

GARANTE

STRUTTURA OFS



ORGANIGRAMMA OFS PRIVACY



L'INTERESSATO

L'Interessato è il soggetto dei dati, ossia la persona fisica alla quale i dati personali si riferiscono.

E' un "**soggetto di diritti**". E' il "**proprietario dei dati personali**".

CHI NON E' UN INTERESSATO (Allo stato attuale della normativa): una persona giuridica, Ente o Associazione.

DIRITTI DELL'INTERESSATO:

Ha il diritto di **conoscere come i dati verranno utilizzati** (art. 13) ed **esprimere il consenso** o meno a questo utilizzo (art. 23).
Ha il diritto di **accedere ai dati**, cioè di esaminare i dati per verificarne l'accuratezza (art. 7: origine dei dati, finalità, modalità di trattamento, estremi del Titolare e del/dei Responsabile/i, soggetti ai quali possono essere comunicati).
Ha il diritto alla **rettifica o aggiornamento**.
Ha il **diritto all'oblio** (2106/679/UE: Diritto alla cancellazione dei dati non pertinenti, non più finalizzati, revocarne il consenso, salvo altri motivi legittimi prevalenti (difesa, cronaca).

IL TITOLARE

Art. 4 c. 1 lett. f

Persona fisica, giuridica, pubblica amministrazione, ente o associazione a cui **compete la decisione circa le finalità, le modalità e gli strumenti per il trattamento**

E' colui che stabilisce **cosa fare con i dati, come farlo, con quali mezzi, come proteggerli.**

La Qualità di Titolare **discende direttamente dai poteri esercitati sui dati**, non è liberamente determinata.

IL RESPONSABILE
del trattamento

Art. 4 p.8 GDPR
Art. 4 c. 1 lett. G DLgs 196/03
Art. 29 DLGS 196/03

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che tratta dati personali per conto del titolare del trattamento**.

La nomina (**per iscritto**) deve essere fatta secondo requisiti di legge in ordine alla "**garanzia di competenza**".

E' solo "Esterno" (Interno = Delegato al trattamento = Incaricato)
Concorre con il Titolare nella responsabilità verso il Garante e l'interessato.

Il Titolare ha il **dovere del Controllo** (art. 32 let. d)

L'INCARICATO

Art. 4 c. 1 lett. h
Art. 30

Persona fisica **autorizzata a compiere operazioni di trattamento dei dati** dal titolare o dal responsabile.

Dev'essere opportunamente **designato per iscritto individuando l'ambito di trattamento consentito** e deve ricevere **istruzioni specifiche** e opportuna **formazione**.

Compie fisicamente il trattamento, ma non ha poteri decisionali su finalità, modalità, etc.

AMMINISTRATORE di SISTEMA

Provv. Gar. 28.11.2008

Figura professionale (persona fisica), in ambito informatico, **finalizzata alla gestione e alla manutenzione di un Sistema Informativo o di sue componenti.**

Nomina personale, per iscritto, individuando l'ambito di applicazione specifico, requisiti di esperienza e competenza tecnica, affidabilità.

Titolare: compiti di vigilanza e valutazione periodica. Controllo tecnico: gestione dei file di log.

ADS Interno e Responsabile Esterno nel trattamento dei dati informatici.

2016/679/CE

IL RESPONSABILE
della protezione dei dati (DPO)

Nominato, obbligatoriamente, in determinati casi (P.A., trattamento su "larga scala" di dati sensibili e giudiziari, trattamenti che richiedono il controllo regolare e sistematico degli interessati).

Nominato dal Titolare, il quale dovrà fornire le risorse (finanziarie e organizzative) necessarie per adempiere al proprio compito.

Caratteristiche: adeguata conoscenza della normativa, indipendenza decisionale sui trattamenti/dati, senza conflitto d'interessi, competenza tecnico-legale.

Compiti: consulenza sugli obblighi normativi, valutazioni d'impatto, autorizzazione al trattamento, sorvegliare il sistema, fornire pareri, cooperare con l'autorità Garante.

IL GARANTE

Il Garante è un organo collegiale ed autonomo,
che ha il dovere istituzionale di vigilare sui trattamenti effettuati in ambito nazionale.

Il garante può:

Ricevere segnalazioni ed Esposti dagli interessati
Effettuare accertamenti
Comminare sanzioni amministrative
Emanare Provvedimenti prescrittivi

MODALITA' PER UN TRATTAMENTO LECITO E PRINCIPI FONDAMENTALI

TRATTAMENTO LECITO 1/2

Un trattamento dei dati è lecito quando:

Chi effettua il trattamento dà un'informativa (Artt. 13 e 14 GDPR 2016/679) ovvero mette a conoscenza l'interessato di:

- Origine dei suoi dati;
- Le finalità del trattamento (dettagliate);
- Le modalità del trattamento e i tempi di conservazione;
- Se i dati debbano o possano essere comunicati a terzi e/o all'estero;
- Soggetti o categorie ai quali i dati possono essere comunicati
- Chi sia il Titolare e il Responsabile del trattamento;
- Quali siano i diritti dell'interessato e a chi rivolgersi per esercitarli.

Va consegnata **PRIMA** di effettuare le operazioni di trattamento.

TRATTAMENTO LECITO 2/2

Per procedere al trattamento, l'interessato, dopo aver ricevuto l'informativa DEVE ESPRIMERE il suo consenso (Artt. dal 5 al 11 GDPR 2016/679).

Il consenso può essere **orale o scritto** (se dati sensibili/giudiziari).

E' **una forma di "contratto"** tra il Titolare e l'Interessato. Dev'essere, quindi, espresso liberamente e differenziato per tipo di trattamento.

L'interessato **può revocarlo** in qualsiasi momento.

Non serve il consenso se: **pericolo di vita, richiesto per legge, diritto alla difesa, per la esecuzione di un contratto** (ad es. per la fatturazione)

Consenso strumento di garanzia

- Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, **preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici** (ad esempio, selezionando un'apposita casella in un sito web).
- Per trattare i **dati sensibili**, il Regolamento prevede che il **consenso** deve essere anche «**esplicito**».
- Viene **esclusa ogni forma di consenso tacito** (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.
- Il consenso **potrà essere revocato** in ogni momento. I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.
- **I fornitori di servizi Internet e i social media, dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.**

CONSENSO PRIVACY OFS

SARA' PREDISPOSTA LA MODULISTICA PRIVACY A LIVELLO NAZIONAL E DISTRIBUITA A TUTTI I LIVELLI REGIONALI E DI FRATERNITA':

- Informativa Privacy per Professi e Novizi
- Consenso Privacy
- Modulo di «gestione anagrafica»

- L'informativa e il consenso dovranno obbligatoriamente essere firmati da ciascun Professo e Novizio dell'OFS al momento dell'ingresso in Fraternità al momento della compilazione del modulo anagrafico.
- Non potranno essere »gestiti» dati di chi non ha sottoscritto il consenso Privacy
- I documenti, per ora, saranno conservati in Fraternità
- Il modulo anagrafico potrà essere usato anche per l'aggiornamento/rinnovo/verifica dei dati anagrafici in possesso al Consiglio

CONCETTO DI RESPONSABILITA' O ACCOUNTABILITY

ACCOUNTABILITY: LA LEGGE ITALIANA

Art. 2050 Codice Civile. Responsabilità per l'esercizio di attività pericolose.

Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.

ACCOUNTABILITY 2016/679 Artt. 24 (Dimostrabilità) e 82 (Risarcimento): o "**responsabilità verificabile**", comporta l'onere, in capo al Titolare del trattamento di dimostrare l'adozione di tutte le prescrizioni privacy (v. CC art. 2050 e art. 15 Dlgs 196/03). I dati sono trattati sotto la responsabilità del Titolare, che assicura e comprova, per ciascuna operazione, la conformità alle disposizioni del regolamento.

RISCHI
e
SANZIONI

OBBLIGO DI NOTIFICA IN CASO DI VIOLAZIONI

(Personal Data Breaches)

GDPR 2016/679 artt. 33 e 34

Viene introdotto l'obbligo di notifica in caso di violazione dei dati personali con grave pregiudizio per quest'ultimi. A data all'Autorità Garante entro 72 ore la quale prescriverà eventualmente l'obbligo di comunicare l'accaduto anche agli interessati.

Problemi: Immagine, class-action (legali), responsabilità dirette e indirette del Titolare/Responsabile/Incaricato, posto di lavoro.

SANZIONI FINO AL 4% DEL FATTURATO MONDIALE ANNUO

Articolo 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie

- <*omissis*>
- In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie **fino a 10 000 000 EUR**, o per le imprese, **fino al 2 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore <*omissis*>
- In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a **20 000 000 EUR**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore<*omissis*>
- 6.In conformità del paragrafo 2 del presente articolo, **l'inosservanza di un ordine da parte dell'autorità di controllo** di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie **fino a 20 000 000 EUR**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore.

SANZIONI AMMINISTRATIVE

TIPOLOGIE	SANZIONI
Omessa o inidonea informativa all'interessato	da € 6.000-18.000 dati sensibili/giudiziari da 8.000-30.000
L'omessa o incompleta notificazione al Garante	da € 10.000-60.000 pubblicazione su uno più giornali
L'omessa informazione o esibizione documenti richiesti dal Garante	da € 6.000-24.000 Euro pubblicazione del provvedimento
La violazione delle disposizioni in materia di cessione dei dati	da € 6.000-8.000 Euro

MISURE di PROTEZIONE

SICUREZZA DEI DATI PERSONALI

Per garantire che le informazioni siamo trattate in modo adeguato la Legge ha introdotto le misure di sicurezza con la finalità di pervenire i rischi di:

1. Distruzione / perdita dei dati
2. Trattamento non consentito
3. Accesso non autorizzato ai dati
4. Trattamento non conforme alla finalità della raccolta

MISURE FISICHE

ORGANIZZATIVE	FISICHE	LOGICHE
•Istruzioni agli incaricati per la segretezza/custodia delle password •Obbligo di non lasciare incustodito ed accessibile lo strumento elettronico •procedure per la custodia di copie di sicurezza •Regolamento uso Sistema Informatico Regolamento uso Tablet/Smarthone	•Ingresso controllato •Registrazione degli accessi •Vigilanza della sede •Custodia in armadi •Continuità dell'alimentazione elettrica •Dispositivi antincendio	•Controllo aggiornati antivirus •Cifratura dei dati memorizzati/trasmessi •Rilevazione delle intercettazioni •Verifiche automatizzate dei requisiti dati

LE MISURE DI SICUREZZA

<u>Misure Minime</u> –
definite esplicitamente nel testo normativo
DISCIPLINARE TECNICO – (Allegato B) del Codice

Un livello essenziale, costituto dalle misure minime, la cui violazione comporta l'applicazione di sanzioni penali

<u>Misure di protezione idonee</u>
tutte quelle che secondo l'evoluzione della tecnologia, **in relazione al tipo di trattamento effettuato e di dati trattai**, debbono essere prese dal Titolare per ridurre i rischi incombenti sui dati. Vanno verificate ed aggiornate periodicamente.

La violazione determina l'illiceità del trattamento, con le relativa conseguenze civilistiche, anche in termine di risarcimento del danno

GDPR 2016/679 – Art. 32
LE MISURE DI SICUREZZA

Tenendo conto dello **stato dell'arte** e **dei costi** di attuazione, nonché della **natura**, dell'**oggetto**, del **contesto** e delle **finalità** del trattamento, come anche del **rischio di varia probabilità e gravità** per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la **pseudonimizzazione** e la **cifratura** dei dati personali;

GDPR 2016/679 – Art. 32
LE MISURE DI SICUREZZA

b) la capacità di **assicurare** su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi e dei servizi di trattamento;

c) la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

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

GDPR 2016/679 – Art. 32
LE MISURE DI SICUREZZA

2.Nel valutare l'adeguato livello di sicurezza, **si tiene conto in special modo dei rischi** presentati dal trattamento che derivano in particolare dalla **distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati**.

3.L'adesione a un **codice di condotta** approvato o a un meccanismo di **certificazione** approvato può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4.Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali **non tratti tali dati se non è istruito in tal senso** dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

MISURE MINIME INFORMATICHE

- Autenticazione informatica
- Gestione delle credenziali di autenticazione;
- Utilizzo di un sistema di autorizzazione
- Altre misure di sicurezza (fisiche e logiche)
- Salvataggio di copie con sistema e frequenza adeguate
- Salvataggio dei file di Log;
- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli

AZIONE
e
ORGANIZZAZIONE

SGP: STATO DELL'ARTE

IERI	OGGI	DOMANI
DPSS NOMINA INCARICATI INFORMATIVE MISURE MINIME IT	PROFILI RESP.TA' AGG. NOMINE DETTAGLIATE ADS ISTRUZIONI CORRETTE INFORMATIVE e CONSENSI CORRETTI REGOL. USO SISTEMI INFORMATIVI REGOL. PERSONALE VIDEOSORVEGLIANZA CONTROLLO EMAIL E INTERNET MISURE TECNICHE NECESSARIE	IMPIANTO DOCUMENTALE E ORGANIZZATIVO INTEGRAZIONE SGQ INTEGRAZIONE 231 MANUALE PROCEDURALE EVIDENZE CORRETTA APPLICAZIONE NORME MISURE TECNICHE ADEGUATE **Principio di** **RENDICONTAZIONE**

IL SISTEMA di GESTIONE PRIVACY

PROCEDURALI	DOCUMENTALI	FISICO/LOGICHE
Insieme di Procedure organizzative Aziendali, integrate con Qualità (SGQ) e 231/01 (Resp. Amm.va d'Impresa), riguardanti: Personale, Commerciale, IT, Gestione Ordini, Progetti, Copyright, Sistemi di Controllo, etc.	Insieme delle evidenze documentali che mirano alla corretta informazione, alla legittimità del trattamento, alle nomine interne ed esterne, alla Formazione, all'evidenza del funzionamento del SGP (Rendicontazione)	Misure poste a protezione delle sedi aziendali, alla gestione ed archiviazione dei documenti, alla gestione della Sicurezza IT, all'integrazione delle "misure minime" ed "idonee"

DOCUMENTALI e PROCEDURALI

D.Lgs 196/03 e 2016/679/CE:

- **Documento Privacy** (o Documento di gestione del Sistema Privacy Aziendale)
- **Manuale Operativo Privacy** (o raccolta delle Procedure Privacy Aziendali)
- **Regolamenti relativi ai Sistemi di Controllo** (Informatico, Videosorveglianza, Tablet/Smartphone, Aule Informatiche, Navigazione Web, etc.)
- **Norme Regolamentari Comportamentali** rispetto alla gestione e al trattamento dei dati personali
- **Gestione Area Informatica** (ADS, Web, Trasparenza, etc.)

Quindi…

qualsiasi organizzazione (pubblica, privata, ente, associazione, religiosa e non, partito/associazione politica, etc.) che tratta dati personali per una qualsiasi finalità (ovvero per un qualsiasi motivo) deve preoccuparsi di averli raccolti e di usarli:

1. solo per le finalità espressamente dichiarate
2. che tali finalità siano legittime
3. che solo le persone effettivamente autorizzate possano usarli
4. che vengano responsabilizzati gli eventuali soggetti esterni chiamati ad usarli in nome e per conto dell'organizzazione
5. che siano tenuti dei registri (costantemente aggiornati) che ne documentino l'uso
6. che vengano adeguatamente protetti e/o custoditi
7. che siano adottate adeguate misure di sicurezza (e che siano documentate) a loro protezione
8. che siano adottate specifiche procedure in caso di violazione, perdita o furto degli archivi custoditi
9. che sia nominata una specifica figura responsabile della protezione dei dati (DPO) a livello di Ordine Nazionale

DOCUMENTI PRIVACY OFS - NAZIONALE -

1. Registro dei trattamenti del Titolare
2. Lettere di nomina delle seguenti figure:
   a. Titolare del trattamento (Ministro Nazionale)
   b. Delegato Privacy Nazionale (che si raccordi con il DPO per qualsiasi problematica Privacy interna all'Ordine)
   c. Incaricati (singoli Consiglieri componenti il Consiglio Nazionale)
   d. Delegati Regionali
3. Procedura di valutazione dei Responsabili
4. Procedura di Data Breach (procedura da attuarsi in caso di violazione dei dati)
5. Procedura di gestione della documentazione cartacea
6. Eventuali Procedure che coinvolgano la Segreteria Nazionale (ad es.: Disciplinare Informatico, etc.)
7. "Manuale d'uso e comportamentale Privacy" prescrittivo per tutti i livelli di Fraternità, con istruzioni semplici e chiare alle quali i Ministri dovranno scrupolosamente attenersi

ATTIVITA' PRIVACY OFS - NAZIONALE -

1. Gestione delle nomine dei Delegati Regionali (Ministri Regionali) e loro conservazione/rinnovo
2. Gestione delle Misure di Sicurezza relative alla sede nazionale ed al sistema informatico interno
3. Gestione della verifica periodica della modulistica utilizzata da tutto l'OFS (con supporto del DPO ed eventuale Legale specializzato)
4. Verifica periodica dei Responsabili esterni
5. Gestione delle richieste per l'esercizio dei diritti ex artt. 15-22 GDPR (per il livello nazionale ed eventualmente regionale), coinvolgendo anche il DPO
6. Valutazione d'impatto relativa alla piattaforma online
7. Altre attività specifiche da individuarsi in sede di analisi di dettaglio

DOCUMENTI PRIVACY OFS - REGIONALE -

1. Lettere di nomina delle seguenti figure:
   a. Incaricati (singoli Consiglieri componenti il Consiglio Regionale)
   b. Delegati di Fraternità
2. Procedura di valutazione dei Responsabili (semplificata e tratta da quella nazionale. Solo se esistenti)
3. Procedura di Data Breach (consistente nel semplice obbligo di contatto tempestivo con il DPO, il quale prenderà il controllo della situazione in nome e per conto del Nazionale)
4. Procedura di gestione della documentazione cartacea
5. Eventuali Procedure che coinvolgano la Segreteria Regionale (ad es.: Disciplinare Informatico, etc.)

ATTIVITA' PRIVACY OFS - REGIONALE -

1. Gestione delle nomine dei Delegati di Fraternità (Ministri di Fraternità) e loro conservazione/rinnovo
2. Gestione delle Misure di Sicurezza relative alla eventuale sede regionale ed al sistema informatico interno
3. Verifica periodica dei Responsabili esterni a livello regionale (Solo se esistenti)
4. Gestione delle richieste per l'esercizio dei diritti ex artt. 15-22 GDPR (per il livello regionale e locale), coinvolgendo eventualmente anche il DPO
5. Altre attività specifiche da individuarsi in sede di analisi di dettaglio

DOCUMENTI PRIVACY OFS – FRATERNITA' -

1. Lettere di nomina delle seguenti figure:
   a. Incaricati (singoli Consiglieri componenti il Consiglio di Fraternità)
2. Procedura di Data Breach (consistente nel semplice obbligo di contatto tempestivo con il DPO, il quale prenderà il controllo della situazione in nome e per conto del Nazionale)
3. Procedura di gestione della documentazione cartacea
4. Eventuali Procedure che coinvolgano la Segreteria Locale (ad es.: Disciplinare Informatico, etc.)
5. Scheda anagrafica di appartenenza alla Fraternità Locale
6. Informative e consensi dei Novizi e dei Professi

ATTIVITA' PRIVACY OFS – FRATERNITA' -

1. Gestione delle Informative e consensi dei Novizi e dei Professi e loro conservazione/rinnovo
2. Gestione ed aggiornamento delle Schede anagrafiche di appartenenza alla Fraternità Locale dei singoli Novizi e Professi
3. Gestione delle Misure di Sicurezza relative alla eventuale sede locale ed al sistema informatico interno
4. Gestione delle richieste per l'esercizio dei diritti ex artt. 15-22 GDPR (semplificata. Qualora pervengano devono interessare immediatamente il Ministro Regionale o un Consigliere Regionale appositamente incaricato)

COSA FARE E COME COMPORTARSI

Regole d'ordinaria diligenza 1/3

1. **Lettera d'incarico** al trattamento dei dati personali (ambito di legittimità; è la"patente")
2. Una volta ricevuta la lettera di nomina e la conseguente autorizzazione, l'Incaricato può svolgere materialmente il trattamento attenendosi alle istruzioni operative dettate dal Responsabile.
3. **attenersi scrupolosamente alle istruzioni** scritte impartite dai Responsabili
4. **osservare i criteri di riservatezza**
5. **trattare i dati in modo lecito** e secondo correttezza
6. **trattare i dati per un periodo di tempo non superiore a quello necessario** agli scopi per i quali sono stati raccolti o successivamente trattati
7. **Porre in essere misure tecniche e organizzative a protezione dei dati della Fraternità (Digitali e Cartacei), anche a livello personale.**
8. **Proteggete adeguatamente i Vostri Computer**

Regole d'ordinaria diligenza 2/3

1. **Far compilare il Modulo Anagrafico e il Consenso Privacy**
2. **Far sottoscrivere ai component del Consiglio le Lettere di Nomina ad incaricato**
3. **non divulgare a terzi estranei** le informazioni di cui si viene a conoscenza
4. **adoperarsi affinché terzi, fraudolentamente, non entrino in possesso di dati** deliberatamente comunicati ("Ruolo attivo" del personale". Ad. es. custodia notebook e documenti cartacei se fuori dalla sede)
5. **non fare copie, per uso personale,** dei dati su cui svolgono operazioni in nome e per conto della Fraternità, se non autorizzati

Regole d'ordinaria diligenza 3/3

5. I documenti contenenti dati personali particolari, **devono essere custoditi in modo da non essere accessibili a persone non incaricate** del trattamento (es. armadi o cassetti chiusi a chiave)
6. I dati personali **non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento dei propri servizi alla Fraternità** (anche se queste persone sono a loro volta incaricate del trattamento).
7. **I dati non devono essere comunicati all'esterno** dell'Ordine e comunque a soggetti terzi **se non previa autorizzazione** (anche generale).
8. **Tenere disponibili I dati di contatto del DPO**

Qualche consiglio…

- Evitare il “fai-da-te” e/o il “copia-incolla” da internet, sempre estremamente rischioso
- Rivolgersi per ogni questione Privacy, alla Segreteria Nazionale che vi metterà in contatto con il DPO
- Farsi aiutare da Professi con capacità informatiche, anche minimali, nella gestione delle informazioni
- Mai sottovalutare richieste e/o incidenti che coinvolgono dati e informazioni dei Fratelli e delle Sorelle, piuttosto: chiedere!!!

GRAZIE

ANDREA PARO
Consulente Privacy certificato TUV CP_26
Associato ANIP (ass. Albo Naz.le Informatici Professionisti)
Codice Nr. 2685 e Certificazione Liv. 5 Professional Partner ANIP
Attività svolte ai sensi della L. 4/2013
paro@geminiconsult.it - Cell. 348.7427151