Trattamento dei dati personali nel rispetto della normativa sulla privacy

Corso APEO

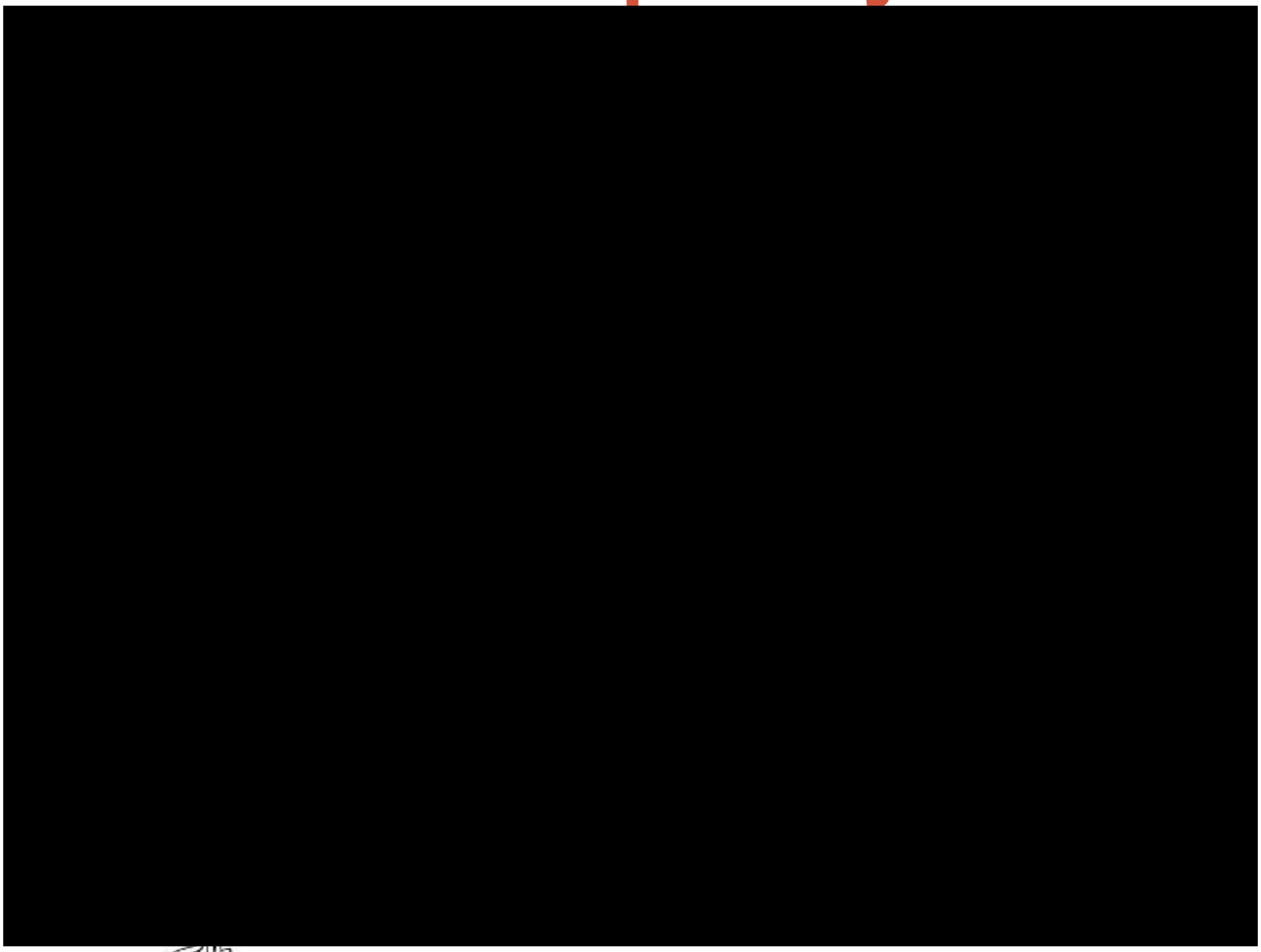
Milano – 20 maggio 2018

APEO
ASSOCIAZIONE PROFESSIONALE
DI ESTETICA ONCOLOGICA

Dr. Giacomo ANDREAZZA

Data Protection Officer

Cos’è la privacy?



Di cosa stiamo parlando?

GDPR 679/2016

- Entrerà in vigore dal 25 maggio 2018
- Sostituisce integralmente D.Lgs. 196/2003
- Nuova regolamentazione uniforme nell'Unione Europea per il trattamento dei dati (privacy) delle persone fisiche

ALCUNE DEFINIZIONI ….

Oggetto della disciplina

- **DATI PERSONALI**

Qualsiasi informazione riguardanti una persona fisica identificata o identificabile.

- **DATI SENSIBILI (categorie particolari di dati)**

Informazioni idonee a rivelare origini razziali, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale e politica, dati relativi alla vita sessuale ed agli orientamenti sessuali, dati relativi alla salute.

Soggetti coinvolti

- **INTERESSATO**

  Persona fisica a cui si riferiscono i dati del trattamento

- **TITOLARE**

  Persona fisica o giuridica che determina le finalità e le modalità del trattamento dei dati

- **RESPONSABILE**

  Persona fisica o giuridica che tratta i dati per conto del titolare

Attività

- **TRATTAMENTO**

  Qualsiasi operazione applicata ai dati personali quali la **raccolta**, la registrazione, la **conservazione**, la **consultazione** e l'uso, la comunicazione e la **diffusione** e la distruzione/**cancellazione**.

PRINCIPI della DISCIPLINA

PRINCIPI «STORICI»

- Liceità
- Correttezza
- Trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità
- Riservatezza

PRINCIPI della DISCIPLINA

PRINCIPI «INNOVATIVI»
(cardini nuova disciplina)

- Accountability (responsabilizzazione)
- Tracciabilità

CATEGORIE DATI TRATTATI NELL'ATTIVITA' DI ESTETISTA

- Dipendenti e collaboratori
- Clienti

DATI CLIENTI

- **Identificativi** (nome, cognome)
- **Dati di contatto** (indirizzo, numero di tel. mail, social)
- **Dati sensibili** (condizioni di salute, patologie ecc.)

Il trattamento dei dati personali (identificativi e di contatto) richiede **l'INFORMATIVA** all'interessato.

Il trattamento dei dati sensibili richiede il **CONSENSO** dell'interessato.

INFORMATIVA

Documento con il quale si forniscono all'interessato le seguenti informazioni

- Identità e dati di contatto del **TITOLARE** del trattamento (estetista o centro estetico)
- **Finalità** del trattamento
- **Persone e/o categorie di persone** che possono venire a **conoscenza dei dati**
- **Periodo** di conservazione dei dati
- Diritti dell'**INTERESSATO**
- **Obbligatorietà** (o meno) del conferimento dei dati

CONSENSO

Approvazione espressa per iscritto del trattamento dei dati sensibili.

- Il consenso deve essere personale, libero e informato.
- Evidenza dell'approvazione del trattamento (sottoscrizione, spunta o altro).

UNA VOLTA RACCOLTI I DATI COSA NE FACCIAMO?

Devono essere conservati e trattati nel rispetto dei principi del regolamento e dei diritti dell'INTERESSATO.

RESPONSABILITA' e TRACCIABILITA'
Vere innovazione del GDPR

- Passaggio da **misure MINIME** a **misure ADEGUATE**

- Predisposizione dei trattamenti sulla base delle **condizioni specifiche** di ogni **attività** ed **organizzazione.**

IN PRATICA……

- I dati possono essere **trattati solo** dal **TITOLARE**, **RESPONSABIL**E e/o da eventuali **incaricati**
- **Formalizzazione dei ruoli** tramite **contratto** e **lettera di incarico** (se necessario piccolo **organigramma privacy**)
- Adeguamento dei **contratti con i for**nitori
- **Minimizzazione** della raccolta dati

IN PRATICA…..

- **Divieto di cessione** o comunicazione dei dati a **terzi** (senza espresso consenso).
- **Riservatezza luoghi** promiscui (es. sala d'attesa).
- **Riservatezza** nelle **comunicazioni.**
- Rispetto **riservatezza professionale** soprattutto con riferimenti ai dati sensibili.

IN PRATICA…..

- Particolare attenzione alla **sicurezza informatica e logica**:
  - Antivirus
  - Backup
  - Firewall
  - Nome Utente e password personale
  - Attenzione a mail sospette!!
- Prevedere la possibilità che gli **INTERESSATI** possano esercitare i loro **diritti**:
  - accesso,
  - rettifica,
  - Oblio,
  - portabilità
- Meccanismo di **cancellazione automatica** dati inutilizzati

UNA MISURA PER TUTTI:
Data Breach

In caso di violazione dei dati personali e sensibili

- **Segnalazione** entro 72 ore al **Garante** della Privacy
- **Comunicazione** agli **interessati**

Ipotesi di violazione

- **Accesso abusivo** ai dati
- **Furto**, **incendio e danneggiamento** supporti materiali
- **Violazione informatica** del sistema operativo
- **Smarrimento** e furto device

MARKETING

Utilizzazione dati raccolti

- Previsione espressa nell'**informativa**
- **Consens**o per marketing diretto (telefonate registrate, sms, mail)
- Meccanismo **«non opposizione»** per vendita propri **prodotti o servizi analoghi** a quelli già venduti
- **Divieto** di **comunicazioni anonime** (numero privato)
- **Consens**o espresso per **trasferimento dati a terzi**.
- Assoluto **divieto cessione** dei **dati sanitari**

SITO WEB e PAGINE SOCIAL

Sito compliance rispetto normativa privacy

- **Informativa** ed eventuale **consenso** se raccoglie e tratta dati personali o sensibili
- **Cookies** (competenza gestore del sito)
- Attenzione alle **fotografie**!! Evitare immagini riconoscibili di pazienti (ed anche collaboratori…)

VIDEOSORVEGLIANZA

- Lecita solo per finalità di **sicurezza** e **tutela del patrimonio**
- Divieto di utilizzo per **controllo a distanza lavoratori**
- Adeguatamente **segnalato con vignetta** conforme alla normativa
- Limitazione dell'accesso alle immagini a persone autorizzate (**credenziali personali**)
- Meccanismi di **cancellazione o sovraregistrazione** automatica nel rispetto dei **termini posti dalla legge**
- **Gestore del sistema** compliance rispetto alla normativa privacy

SANZIONI

- **CIVILI**

Responsabilità nei confronti degli interessati per i danni patrimoniali e non patrimoniali ai sensi dell'art. 2050 c.c. (attività pericolosa, inversione onore probatorio)

- **AMMINISTRATIVE**

Sanzioni da 10 a 20 milioni di euro (o da 2% al 4% del fatturato mondiale)

- **PENALI**

Reclusione da 6 mesi a 3 anni per trattamenti illeciti, col dolo specifico di trarre per sé o per altri un ingiusto profitto o causare ad altri un danno o per false dichiarazioni al Garante

RESPONSABILITA' CIVILE

RESPONSABILITA' CIVILE (art. 2043 c.c.)

- Dolo o colpa
- Danno ingiusto
- Danno conseguenza
- Rapporto di causalità tra azione (o omissione) e danno ingiusto e tra questo e il danno conseguenza
- Prescrizione 5 anni
- Onere probatorio in capo al danneggiato
- Responsabilità anche per collaboratori e dipendenti (art. 2049 c.c.)

RESPONSABILITÀ PROFESSIONALE

RESPONSABILITÀ PROFESSIONALE (artt. 2222 e 1218 c.c.)

- Rapporto contrattuale
- Prova liberatoria solo causa non imputabile
- Prescrizione 10 anni
- Onere di allegazione in capo al danneggiato
- Adempimento della prestazione con correttezza e secondo regole dell'arte
- Adozione di prudenza, perizia e rispetto di linee guida e buone pratiche
- Responsabilità anche per l'attività di collaboratori e dipendenti (art. 1228 c.c.)

Grazie per l'attenzione