La riforma della Privacy
il nuovo Regolamento europeo

Assemblea Nazionale

Rimini, 2-3-4 Maggio 2018

La Privacy

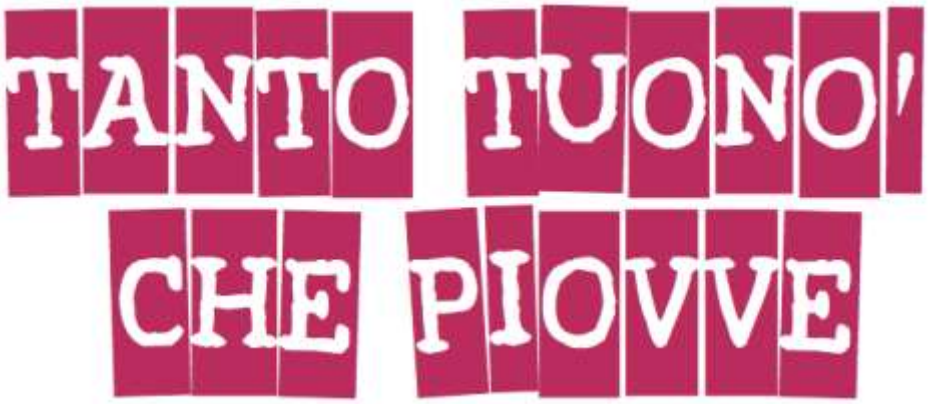
Il termine ***privacy*** indica
il diritto alla riservatezza della vita privata di una persona

Il Codice della Protezione dei Dati Personali ha radici
nell' ambito di disposizioni comunitarie
la **direttiva comunitaria 95/46 - "direttiva madre"**
è il testo di riferimento in materia privacy per gli stati membri.

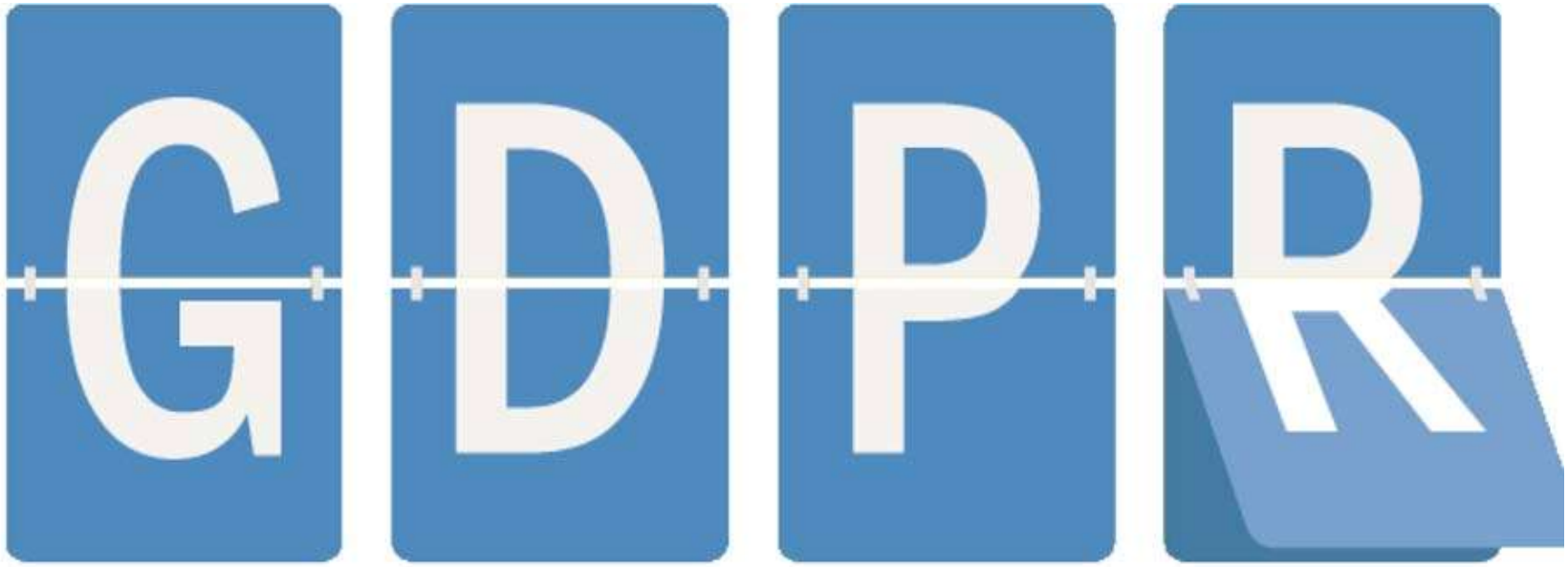
Con il mercato digitale gli **scenari sono molto diversi**
Una riforma generale della normativa sulla protezione dei dati personali era **indispensabile per regolamentare i flussi** che attraversano il pianeta

=

fondamentale conseguire
un unico strumento normativo all'interno dell'UE



dopo un iter legislativo durato 4 anni è arrivato
il **nuovo Regolamento dell'Unione Europea sulla protezione dei dati**
vigente nell'area UE
e che in Italia prenderà il posto
del "vecchio" Codice della Privacy (Dlgs 196/2003)



A seguito della pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea del 4 giugno 2016**, è entrato formalmente in vigore il 24 maggio 2016 il Regolamento Europeo per la Protezione dei Dati Personali 2016/679** o nella sua accezione inglese **General Data Protection Regulation (GDPR)**

Quadro legislativo comune ed omogeneo in materia di protezione dei dati personali e di libera circolazione dei dati

Attualmente vi sono 27 differenti normative in materia

Trattandosi di **Regolamento** e *non di Direttiva,*
non sarà soggetto a recepimento,
quindi gli stati membri non potranno "adattare" (modificare")
il quadro normativo, che sarà quindi omogeneo per tutti

KEEP
CALM
AND
PREPARE FOR
THE GDPR

Opportunità e limiti del GDPR

Che significa? **RESPONSABILIZZARE.**

Il Regolamento ha uno stampo «*europeo*» molto diverso dal Codice Privacy italiano.

Ogni soggetto dovrà autonomamente scegliere come ed in che misura mettere in sicurezza i trattamenti (antivirus, sistemi di salvataggio e cancellazione dei dati..)

N.B. AMPLIATA LA LIBERTA' E LA DISCREZIONALITA'

Principio di accountability

Il titolare del trattamento deve mettere in atto adeguate misure tecniche ed organizzative, per **garantire** ***ed essere in grado di dimostrare*** che le operazioni di trattamento vengono effettuate in conformità alla nuova disciplina.

Il potere decisionale riguarda le *finalità* ed i *mezzi*.
Significa determinare il «**perché**» e il «**come**» del trattamento

Per mantenere la sicurezza e prevenire trattamenti in violazione al regolamento, **il titolare o il responsabile del trattamento dovrebbero valutare i rischi** inerenti al trattamento e attuare misure per limitare tali rischi.

Nella valutazione del rischio per la sicurezza dei dati è opportuno **tenere in considerazione i rischi presentati dal trattamento** dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Termini e Definizioni

Un **dato personale** è
Qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato») tramite ulteriori dati.

Possibili identificativi
- il nome
- i dati relativi all'ubicazione
- un identificativo online
- uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica (dati biometrici)
- uno o più elementi caratteristici della sua identità economica, culturale o sociale

Dato sensibile

Qualunque dato che può rivelare l'origine razziale, etnica, le convinzioni religiose, le opinioni politiche, **l'appartenenza a** partiti, **sindacati o associazioni**, lo stato di salute e la vita sessuale.

Divieto di trattare i dati sensibili

ART. 9 Regolamento - eccezione al divieto

Il divieto non si applica se il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da **una associazione che persegua finalità sindacali**, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con l'associazione a motivo delle sue finalità e **a condizione che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato**

Trattamento dei dati personali:
Qualsiasi operazione che può essere effettuata utilizzando dati personali delle persone:

- la raccolta
- la registrazione
- l'organizzazione
- la strutturazione
- la conservazione
- la modifica
- l'estrazione
- la consultazione
- l'uso
- la limitazione
- la cancellazione
- la distruzione.

CISL SCUOLA

Il potere di determinare il flusso delle proprie informazioni

Il regolamento supera la concezione statica e «proprietaria» dei dati personali a favore di un approccio dinamico.

Due macrocategorie di diritti riconosciuti:

- Diritti conoscitivi
- Diritti di controllo

Resi più cogenti e precisati obblighi/procedure per il titolare

Diritti conoscitivi

- Ricevere info sul trattamento: diritto all'informativa
- Ottenere info sul trattamento: diritto di accesso
- Ricevere info sulle violazioni: diritto alla comunicazione di violazioni dati

Diritti di controllo

- Autorizzare il trattamento: diritto al consenso
- Modificare il trattamento: diritto alla limitazione
- Far cessare il trattamento: diritto di opposizione
- Modificare i dati: diritto di rettifica
- Eliminare i dati: diritto di cancellazione/oblio

Il **Consenso dell'Interessato** è qualsiasi **manifestazione dei volontà libera, specifica, informata e inequivocabile** dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile.

Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle.

Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste.

Il Consenso

Cosa Cambia

- **ONERE DELLA PROVA della prestazione del consenso a carico del titolare del trattamento.**

Cosa è Invariato

- **deve essere libero, specifico, informato e inequivocabile**
- **non è ammesso il consenso tacito o presunto**

I soggetti coinvolti

Il **Titolare del Trattamento:** la **persona fisica** o giuridica che, singolarmente o insieme ad altri, **determina le finalità del Trattamento di dati personali e le misure tecniche ed organizzative di adeguamento al Regolamento**

Il **Responsabile del Trattamento**: la **persona fisica o giuridica**, l'autorità pubblica, o altro organismo **che tratta i dati personali per conto del titolare, previo contratto specifico**

La persona autorizzata al Trattamento: il dipendente o il collaboratore che per conto del titolare o del responsabile del trattamento elabora o utilizza materialmente i dati sulla base delle istruzioni ricevute

Il DPO per il Garante

Il Responsabile della protezione dei dati

«a q*uesta figura, saranno affidati* ***compiti sostanziali****, per* ***assicurare*** *il rispetto della* ***normativa*** *in materia di privacy da parte della società o ente nell' ambito del quale viene designato. Sarà affidato a questo nuovo soggetto, dotato di una* ***specifica professionalità*** *nel settore della protezione dei dati personali, il ruolo di "****presidio avanzato****" del rispetto dei princìpi e degli adempimenti in materia nonché di interlocutore ed elemento di connessione tra il titolare del trattamento e l'Autorità*».

Il DPO è obbligatorio

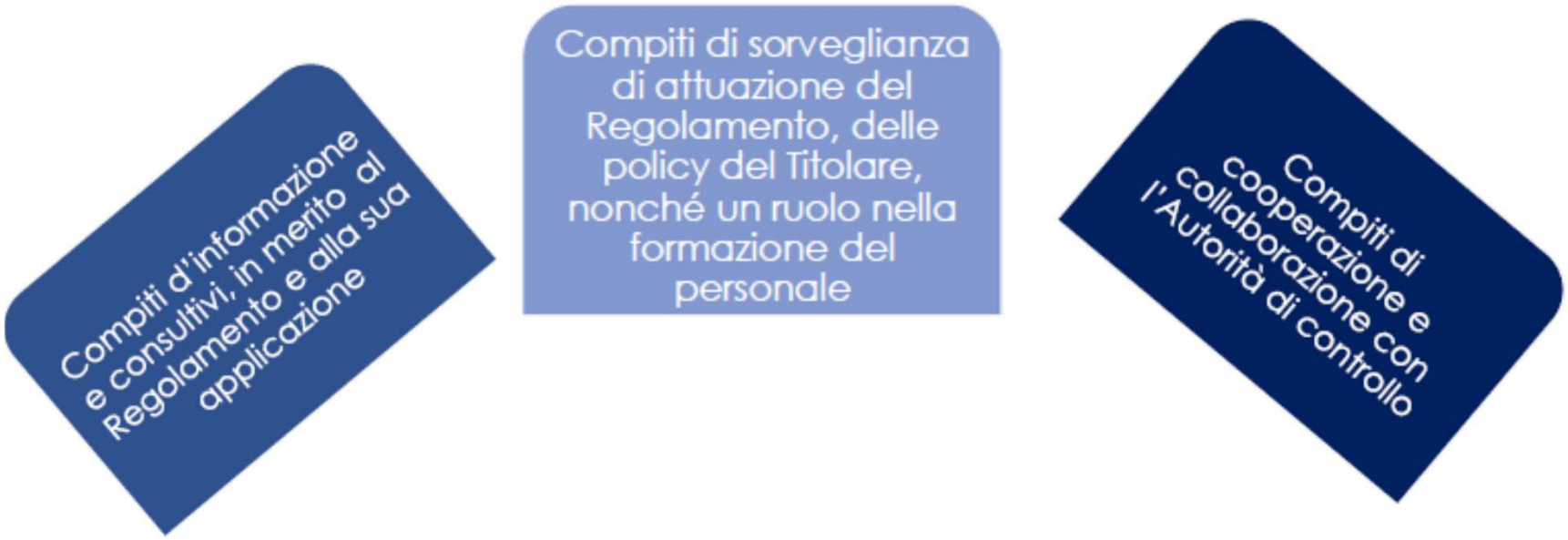
Il Titolare del trattamento e il Responsabile del trattamento sono obbligati a designare un "Responsabile della protezione dei dati" in tre casi, elencati nel paragrafo 1 dell'art. 37, e cioè:

a) se il trattamento è effettuato da un'"autorità pubblica" o da un "organismo pubblico";

b) se le **"attività principali"** del Titolare o del Responsabile del **trattamento** consistono in trattamenti che, per loro natura/ambito di applicazione/finalità, richiedono un **"monitoraggio regolare e sistematico"** degli interessati su **"larga scala"**;

c) se le "attività principali" consistono nel trattamento su **"larga scala" di "categorie particolari" di dati** (c.d. dati sensibili) o di dati personali relativi a condanne penali e reati (c.d. dati giudiziari).

I compiti del DPO



CISL SCUOLA

Più soggetti possono nominare lo stesso DPO ?

Si. L'articolo 37 consente a un gruppo imprenditoriale di nominare un unico DPO a condizione che quest'ultimo sia ***facilmente raggiungibile da ciascun stabilimento.*** L'Autorità di controllo e gli interessati devono poter comunicare (raggiungere) agevolmente con il DPO

La responsabilità

Non gestionale, ma chi risponde in caso di violazione??

Il Titolare o il responsabile mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza.

La sicurezza…

È, prima di tutto, sicurezza delle persone fisiche cioè degli interessati, di cui si trattano i dati personali.

La sicurezza delle reti, degli strumenti, delle tecnologie *non è lo scopo*, **ma lo strumento** della sicurezza delle persone.

Approccio basato sul rischio e responsabilizzazione

Cosa cambia

La valutazione del rischio deve avvenire prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso" - art. 25), e richiede **un'analisi preventiva sugli impatti relativi alla protezione dei dati** e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

La Violazione dei dati personali

La violazione di sicurezza in modo accidentale o illecito

Può provocare danni fisici, materiali o immateriali.

***esempio**:* perdita del controllo dei dati personali, limitazione dei loro diritti, discriminazione, pregiudizio alla reputazione, perdita alla riservatezza dei dati, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati.

Violazione dei dati (data Breach)

Cosa Cambia

- A partire dal 25 maggio 2018, tutti i titolari dovranno **notificare all'autorità di controllo** le violazioni di dati personali di cui vengano a conoscenza, ***"senza ingiustificato ritardo"*, e ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.**

Le sanzioni amministrative

NOVITA': Un'efficace protezione dei dati personali in tutta la UE presuppone la disciplina dei diritti degli interessati, degli obblighi di coloro che effettuano il trattamento e la determinazione di sanzioni amministrative pecuniarie.

Le **sanzioni amministrative** arrivano a colpire Titolari e Responsabili **fino a 20 milioni di euro** nel caso in cui siano violate:

Principi relativi al trattamento ed al consenso

Disposizioni relative ai diritti dell'interessato

Disposizioni in materia di trasferimento dati

Violazione di ordine di cessazione del trattamento

La fissazione dell'importo

Le sanzioni devono essere *in ogni singolo caso effettive, proporzionate e dissuasive*.

Applicazione non meccanica e assoluta, ma ponderata e flessibile.

Criteri attenuanti: le misure di sicurezza adottate e la collaborazione con l'autorità

Il 25 maggio si avvicina..

COSA FARE ADESSO?

Analisi dell'esistente

CHI

Casistica soggettiva: CHI SONO?

Soggetto privato con attività prevalente trattamento di dati sensibili su larga scale

EFFETTI

- Applicazione del consenso
- Obbligo di nomina di un responsabile della protezione dei dati - DPO

Analisi della propria organizzazione

- Quali uffici trattano dati di persone fisiche?
- Iniziare processo di adeguamento al Regolamento
- Seguire le priorità segnalate dal Garante: Designare il Responsabile della protezione dei dati personali - DPO

Modalità operativa

ENTRO IL 25 MAGGIO 2018

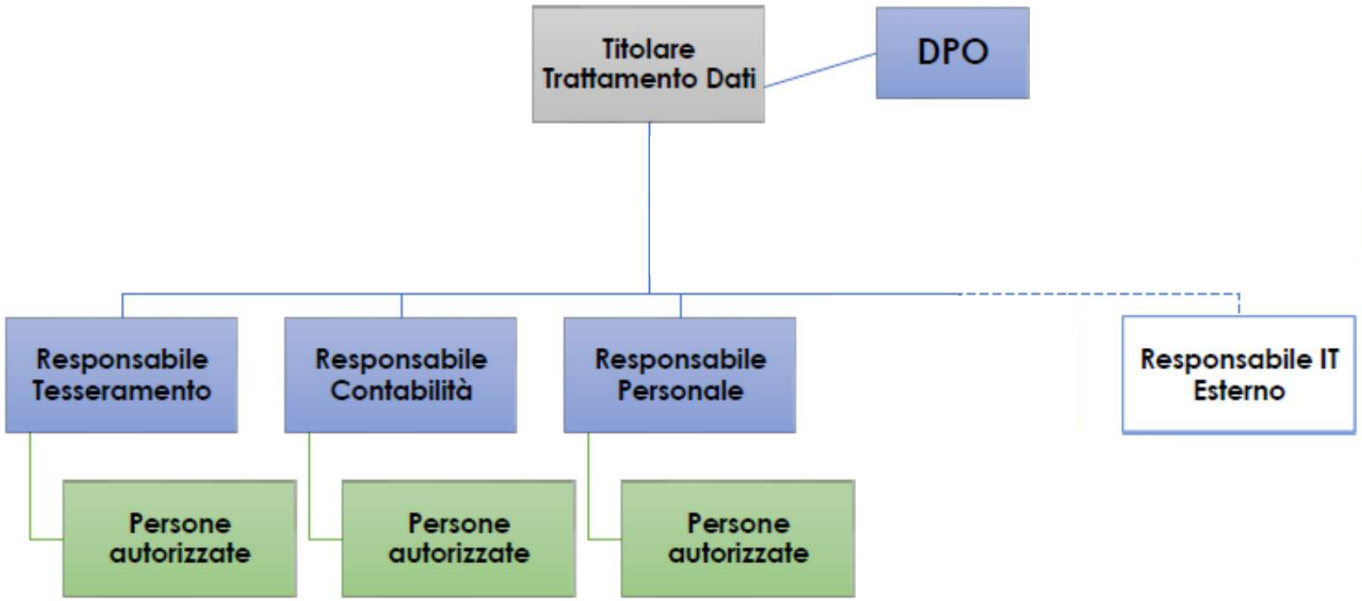
- Individuazione modello organizzativo interno
- Adozione organigramma Privacy
- Rilascio nomine e autorizzazioni
- Comunicazione nomina DPO al Garante

Organigramma privacy

Descrizione delle categorie di:

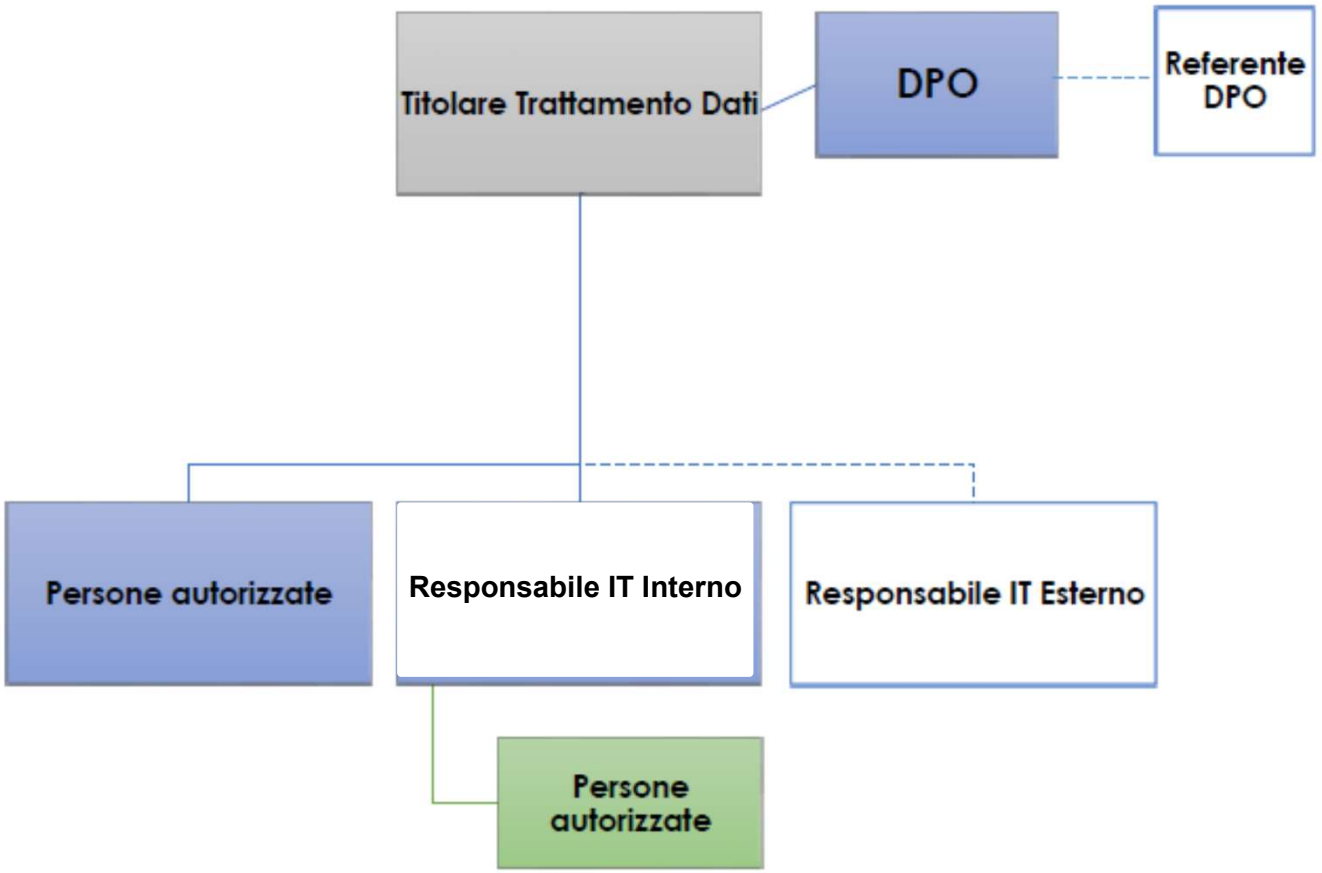
- Titolare del trattamento
- DPO
- Referenti DPO
- Responsabili interni/esterni
- Soggetti autorizzati

Organigramma Struttura 1



CISL SCUOLA

Organigramma Struttura 2



Adempimenti successivi

- Registro del Trattamento
- Adeguamento procedurale
- Gestione ed aggiornamento della contrattualistica
- Linee guida per le modalità di cancellazione e dismissione dei dati

Conclusioni

La CISL è una grande realtà, dove l'autonomia è fondamentale e necessariamente garantita

Ma, lato Privacy occorre regolare i processi: **necessario fissare regole e strumenti comuni** per mettere in sicurezza l'interessato: l'iscritto

Obbiettivo: adottare un approccio culturale al tema Privacy completamente differente

"se il diritto svolge oggi, sempre più, una funzione
di umanizzazione della tecnica,
il diritto alla protezione dei dati rappresenta
una straordinaria risorsa per mantenere la persona,
nella sua libertà e nella sua responsabilità,
al centro della società digitale"

(*Antonello Soro* - presidente Autorità Garante per la Protezione dei Dati Personali)