GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SME Data

ROMA TRE
UNIVERSITÀ DEGLI STUDI

GIURISPRUDENZA
DIPARTIMENTO
DI ECCELLENZA
2018-2022

Training Of Trainers

GOVERNANCE E ACCOUNTABILITY

LUIGI CARROZZI

GARANTE PRIVACY

Indice

Training of Trainers

- Governance della protezione dei dati e principio di accountability nelle organizzazioni.
- Suggerimenti per definire efficaci policy interne per la gestione dei dati personali.
- Ruolo e responsabilità di un DPO nel contesto dei trattamenti delle PMI
- Valutazione dei trattamenti dei dati

Governance della protezione dei dati e principio di responsabilità nelle organizzazioni.

IL CONTESTO DI RIFERIMENTO – OGGETTO E FINALITA' DEL REGOLAMENTO – IL VALORE DA PROTEGGERE

GDPR: il valore da proteggere

Training of Trainers

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO

EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

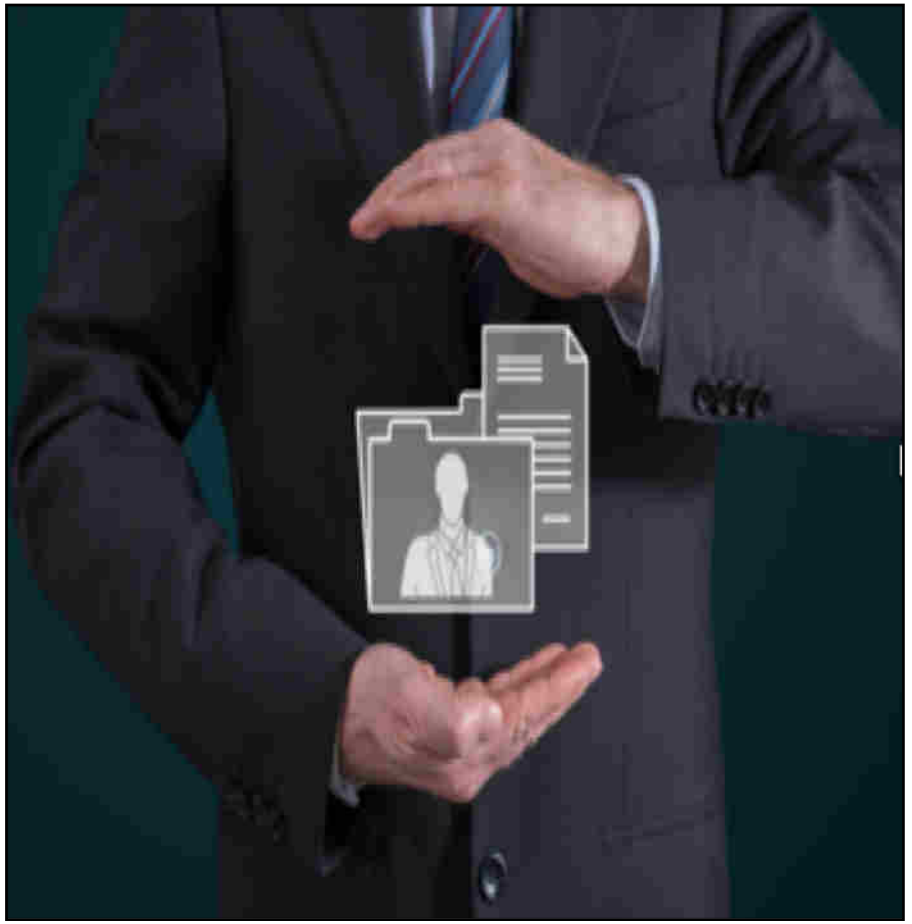
relativo alla protezione delle persone fisiche

con riguardo al trattamento dei dati personali,

nonché alla libera circolazione di tali dati

e che abroga la direttiva 95/46/CE

(regolamento generale sulla protezione dei dati)



GDPR Art. 1) – Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla **protezione delle persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla **libera circolazione di tali dati**

……

Sfide della protezione dei dati personali

Training of Trainers

RGPD – Considerando 6)

- La tecnologia consente di utilizzare dati personali come mai in precedenza
- Crescita della portata della raccolta e condivisione di dati personali
- Le persone fisiche rendono disponibili al pubblico e su scala globale le proprie informazioni personali
- La tecnologia dovrebbe facilitare la libera circolazione dei dati personali

RGPD - CONSIDERANDO 7

- Necessità di un **quadro solido e coerente** di protezione dei dati in UE **affiancato da efficaci misure di attuazione**
- È opportuno che:

  le **persone fisiche** abbiano il controllo dei dati personali che li riguardano

  La certezza giuridica e operativa sia rafforzata tanto per le **persone fisiche** quanto per gli **operatori economici** e le **autorità pubbliche**.

CONCETTO DI ACCOUNTABILITY – IMPLICAZIONI OPERATIVE

Gruppo di lavoro WP29 - WP243 - Linee guida sui responsabili della protezione dei dati

"Il Regolamento generale sulla protezione dei dati…….offre un ***quadro di riferimento in termini di compliance*** *per la protezione dei dati in Europa, aggiornato e* ***fondato sul principio di "responsabilizzazione"*** *(accountability)"*

L’ “Accountability” ai sensi del GDPR

Training of Trainers

L'articolo 5 del RGPD) sancisce i principi del trattamento dei dati personali.

Il paragrafo 1) prevede i principi fondamentali di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, accuratezza, limitazione della conservazione e sicurezza (integrità e riservatezza).

Il paragrafo 2) stabilisce:
"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘**accountability**’).

Responsabilità del titolare del trattamento Art. 24)

Par. 1)

il **titolare del trattamento mette in atto misure tecniche e organizzative adeguate** per

- garantire, ed
- essere in grado di dimostrare,

che il trattamento è effettuato **conformemente al Regolamento**.

Ai fini dell'individuazione di tali **misure** si deve tenere conto

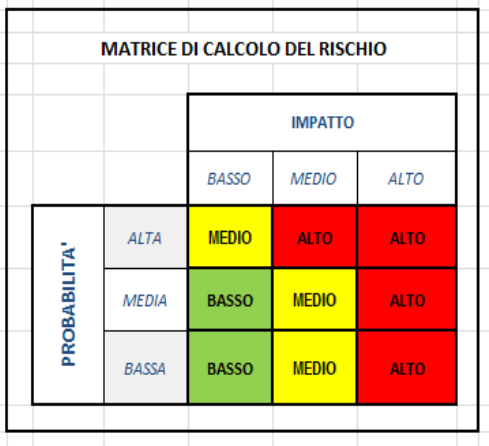
- della **natura**, **dell'ambito di applicazione**, del **contesto** e delle **finalità** del trattamento,
- dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

Par.2)

Se ciò è proporzionato rispetto alle attività di trattamento, **le misure includono l'attuazione di politiche adeguate in** materia di protezione dei dati

Par. 3)

L'adesione ai **codici di condotta** (Art. 40) o a un **meccanismo di certificazione** (Art. 42) può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.



PRIVACY GOVERNANCE

La necessità di una “Privacy Governance”

Training of Trainers

- I titolari del trattamento sono tenuti a porre in essere quanto necessario per **garantire la conformità** delle loro attività di trattamento a tali principi ed a fornirne la prova

- Ciò implica la **capacità di gestire** l'attività in conformità alle disposizioni del RGPD

- È necessario predisporre un **sistema di *governance*** dell’ intero processo di conformità, indipendentemente dalle dimensioni e dall'attività dell'azienda.

Privacy Governance

Privacy Governance I

Training of Trainers

Principali elementi di un sistema di Governance

1. Ove opportuno, identificare **l'organizzazione interna** privacy, nominando un responsabile della protezione dei dati e assegnando ruoli e responsabilità interne

2. Definire ed attuare **Policy** di protezione dei dati

3. Mettere in atto un solido processo di **gestione del rischio** relativo al trattamento dei dati personali facendo riferimento ai diritti e la libertà degli interessati come valore da proteggere

Privacy Governance II

Training of Trainers

4. identificare e attuare **misure di sicurezza** tecniche e organizzative **coerenti ed adeguate**;

5. adottare, su **base continua**, un approccio di "**protezione dei dati fin dalla progettazione e impostazione predefinita**"; questo approccio dovrebbe essere inteso sia per **scopi tecnici** che **organizzativi**

6. **stipulare contratti** con outsourcer o altre organizzazioni che elaborano dati personali per conto del titolare del trattamento;

Privacy Governance III

Training of Trainers

7. creare un **registro delle attività** di trattamento dei dati personali

8. conservare la **documentazione sulle decisioni e azioni** prese sulle operazioni di trattamento effettuate e svolgere, su base regolare, un riesame generale di tali operazioni;

9. adottare un processo di **gestione degli incidenti** al fine di gestire le violazioni dei dati personali secondo le previsioni GDPR

Privacy Governance IV

Training of Trainers

10. quando il trattamento dei dati personali puo comportare un un rischio elevato per i diritti e le libertà delle persone, effettuare una **valutazione d'impatto sulla protezione dei dati**

11. laddove opportuno, aderire a **codici di condotta** e **schemi di certificazione.**

Suggerimenti per definire efficaci policy interne per la gestione dei dati personali.

Policy e Procedure

Training of Trainers

- **Le Policy** sono principi, regole e linee guida formulate e adottate da un'organizzazione per raggiungere i propri obiettivi. Sono generalmente rese note in una forma ampiamente accessibile.

- **Le procedure** sono i metodi specifici utilizzati per tradurre le politiche nelle attività quotidiane dell'organizzazione.

- Le politiche e le procedure sono progettate per indirizzare l'esecuzione e controllare le **principali attività** e le **decisioni** rilevanti di un'organizzazione

RGPD e Policy

- La costituzione di un sistema di policy e procedure **adeguato alla realtà dell'organizzazione,** ben articolato e coerente, può essere di notevole supporto per la conformità al RGPD

- Queste possono includere ad esempio, **policy generali di protezione dei dati** e **policy specifiche** come quelle che regolano i tempi di conservazione dei dati o la gestione della sicurezza delle informazioni

Policy specifiche

Training of Trainers

Es: Policy di sicurezza delle informazioni

- controllo degli accessi
- classificazione e gestione delle informazioni
- utilizzo degli strumenti informatici
- utilizzo delle apparecchiature mobili
- utilizzo e gestione dei media rimuovibili
- utilizzo delle protezioni crittografiche
- backup e ripristino dei dati
- utilizzo di Internet e dei social media
- gestione degli incidenti di sicurezza delle informazioni
- ……

Valore delle Policy

Training of Trainers

L'utilizzo di policy e procedure consente di **rendere disponibili ai dipendenti indicazioni chiare su come procedere in ambiti specifici** di attività, di cosa non è consentito fare e come comportarsi in determinate circostanze.

Indipendentemente dalle dimensioni dell'organizzazione, la definizione e l'implementazione di politiche e procedure documentate;

- **facilita lo svolgimento dei processi** in conformità con il RGPD
- consente di **risparmiare tempo e risorse**
- Riduce la **probabilità** e relative **conseguenze** di incorrere in **violazioni** dei dati personali.
- dimostra che l'organizzazione è ben strutturata nella protezione dei dati personali, ciò incrementa **la reputazione** dell'organizzazione e le opportunità di business

Policy e Procedure: caratteristiche

Training of Trainers

E’ auspicabile sviluppare policy aventi le seguenti caratteristiche.

a. **Allineate all’indirizzo generale di gestione dell'organizzazione**
   Coerenti con la dichiarazione di intenti dell'organizzazione (missione, visione) tenendo conto anche delle altre eventuali policy generali o altre disposizioni già fornite sulle questioni che la policy intende regolare

b. **Correttamente comunicate**
   Fondamentale la comprensione da parte di tutti all'interno dell'organizzazione del motivo per cui la politica è stata sviluppata, quale obiettivo, intende raggiungere una politica, a cosa quando, in quali condizioni si applica, garantendo una comunicazione e una formazione efficace a tutto il personale interessato.

Policy e Procedure: caratteristiche

Training of Trainers

c. **Chiare e coerenti**.

Le policy devono essere espresse mediante dichiarazioni chiare, facili da comprendere e da applicare, giustificabili, efficaci e coerenti con il contesto dell'organizzazione a cui si riferiscono

d. **Aggiornate**.

Le organizzazioni e l'ambiente in cui operano sono molto spesso altamente dinamici; per questo motivo, le politiche devono regolarmente riviste e comunque quando il processo a cui si applicano cambia per condizioni interne o esterne.

Importanti indicazioni possono anche provenire del personale interessato laddove adeguatamente coinvolto nei processi di miglioramento

Ruolo e responsabilità di un DPO nel contesto dei trattamenti delle PMI

Compiti del responsabile della protezione dei dati (Art. 39)

Training of Trainers

Compiti del RPD

1. **informare e fornire consulenza (**al titolare o al responsabile e ai dipendenti)
2. **sorvegliare l'osservanza del Regolamento**,
3. Fornire un **parere** sulla **valutazione d'impatto** sulla protezione dei dati e ne **sorveglia** lo svolgimento;
4. **cooperare** e fungere da **punto di contatto** con **l'autorità di controllo** e con questa

Nell'eseguire i propri compiti il responsabile della protezione dei dati **considera debitamente i rischi inerenti al trattamento**, tenuto conto

- della natura,
- dell'ambito di applicazione,
- del contesto
- delle finalità del trattamento

RGPD - CONSIDERANDO 77

Gli orientamenti per la **messa in atto di opportune misure** e **per dimostrare la conformità** da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda

- **l'individuazione del rischio connesso al trattamento**,
- la sua **valutazione** in termini di **origine**, **natura, probabilità** e **gravità,**
- **l'individuazione di migliori prassi per attenuare il rischio**

potrebbero essere forniti in particolare mediante

a. codici di condotta approvati,
b. certificazioni approvate,
c. linee guida fornite dal comitato **o**
d. indicazioni fornite da un responsabile della protezione dei dati.

……

RPD Compiti

Ruolo nell'informare e fornire consulenza ed indirizzi

- supporto alla raccolta di informazioni per la tenuta del Registro dei trattamenti
- orientamenti per l'individuazione e la valutazione del rischio
- orientamenti per la messa in atto di opportune misure
- orientamenti per dimostrare la conformità

Ruolo nel sorvegliare l'osservanza del RGPD

- la raccolta di informazioni per individuare i trattamenti svolti (Registro dei trattamenti);
- l'analisi e la verifica dei trattamenti in termini di loro conformità

RPD Compiti

Ruolo nella valutazione di impatto sulla protezione dei dati

- Art 35 (2) prevede in modo specifico che il titolare "si consulta" con il RPD quando svolge una DPIA.
- Art. 39 (1)c affida al RPD il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento"

Cooperazione con l'autorità di controllo e funzione di punto di contatto

Ruolo di facilitatore:

- coopera con l'autorità di controllo
- punto di contatto per l'autorità di controllo (ad es, per consultazione preventiva di cui all'articolo 36)
- effettuare, se del caso, consultazioni relativamente a ogni altra questione

Compiti del RPD: guida pratica I

Dal «Manuale del RPD» - Douwe Korff & Marie Georges

Training of Trainers

Manuale del RPD - Douwe Korff & Marie Georges
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9152429

A) Compito preliminare:

Delineare il contesto in cui opera il titolare

B) Funzioni organizzative:

1 - Creazione di un registro delle attività di trattamento
2 - Verifica delle attività di trattamento di dati personali
3 - Valutazione dei rischi posti dalle attività di trattamento di dati personali
4 - Gestione dei trattamenti che possono comportare un "rischio elevato"

Compiti del RPD: guida pratica II

Dal Manuale del RPD - Douwe Korff & Marie Georges

Training of Trainers

C) Controllo della conformità:

5 - Ripetizione dei compiti 1-3 (e 4) su base continuativa

6 - Gestione delle violazioni dei dati personali (data breach)

7 - Compiti di indagine (compresa le gestione dei reclami interni)

D) Funzioni consultive:

8 - Funzioni di consulenza

9 - Sostegno e promozione della “Protezione dei dati dalla fase di progettazione” e della “Protezione dei dati per impostazione predefinita”(Data protection by Design & Default)

10 - Consulenza e monitoraggio della conformità delle politiche di protezione dei dati, dei contratti tra contitolari, tra titolari, e tra titolare e responsabile, norme vincolanti di impresa, e clausole per il trasferimento dei dati.

11 - Coinvolgimento nei codici di condotta e nelle certificazioni

Compiti del RPD: guida pratica III

Dal Manuale del RPD - Douwe Korff & Marie Georges

Training of Trainers

E) Cooperazione con e consultazione dell'Autorità di protezione dati:

12 - Cooperazione con l'Autorità di protezione dati

F) Gestione delle richieste dell'interessato:

13 - Gestione delle richieste dell'interessato

G) Informazione e sensibilizzazione:

14 - Compiti di informazione e sensibilizzazione interna ed esterna

15 - Pianificazione e riesame delle attività del RPD

DPO Conosenze e competenze - Art 37(5)

Training of Trainers

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SME Data

ROMA TRE
UNIVERSITÀ DEGLI STUDI

GIURISPRUDENZA
DIPARTIMENTO
DI ECCELLENZA
2018-2022

Training Of Trainers

VALUTAZIONE DEI TRATTAMENTI DEI DATI

LUIGI CARROZZI

Garante per la protezione dei dati personali

Indice

Training of Trainers

- L’importanza per le PMI di mantenere un registro delle attività di trattamento: ruoli e responsabilità
- Contenuto del registro ai sensi dell'art. 30
- Valutazione del trattamento dei dati - esercizio

Accountability e Registro delle Attivita di trattamento

Training of Trainers

Rendere una entità Accountable significa assegnare compiti da eseguire e decisioni da assumere **e aspettarsi che tale entità risponda del suo operato e delle decisioni prese.**
In questo senso, l'accountability è **l'essere tenuti a rispondere** dei compiti assegnati delle decisioni che ci competono ed **essere in grado di dimostrarlo.**

Il quadro complessivo di conoscenze sui dati personali e delle relative operazioni di trattamento fornito dal Registro, **è il primo passo verso l'accountability,** poiché consente la valutazione del rischio sui diritti e le libertà delle persone e di attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Importanza del Registro

Training of Trainers

RGPD - CONSIDERANDO 82

Per dimostrare che si conforma al presente regolamento**, il titolare del trattamento o il responsabile del trattamento **dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità.

*Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione **affinché possano servire per monitorare detti trattamenti.***

Registro dei trattamenti - Titolare

Training of Trainers

Modello di “registro semplificato” delle attività di trattamento del titolare per PMI

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*							
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*							
TIPOLOGIA DI TRATTAMENTO	**FINALITA' E BASI LEGALI DEL TRATTAMENTO**	**CATEGORIE DI INTERSSATI**	**CATEGORIE DI DATI PERSONALI**	**CATEGORIE DI DESTINATARI** *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**TERMINI ULTIMI DI CANCELLAZIONE PREVISTI**	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

Registro dei trattamenti- Responsabile

Training of Trainers

Modello di “registro semplificato” delle attività di trattamento del responsabile per PMI

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*		
RESPONSABILE *[inserire la denominazione e i dati di contatto]*		
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*		
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*		
CATEGORIA DI TRATTAMENTO	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[Indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

Tenuta del registro dei trattamenti deroga per le piccole e medie imprese

Training of Trainers

RGPD – Articolo 30(5)

Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che:

- *il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato,*
- *il trattamento non sia occasionale o*
- *includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.*

WP29 - POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR

…..la formulazione dell'articolo 30, paragrafo 5, è chiara; i tre tipi di trattamento a cui non si applica la deroga sono in alternativa ("o") e il verificarsi di uno solo di essi innesca l'obbligo di conservare il registro delle attività di trattamento

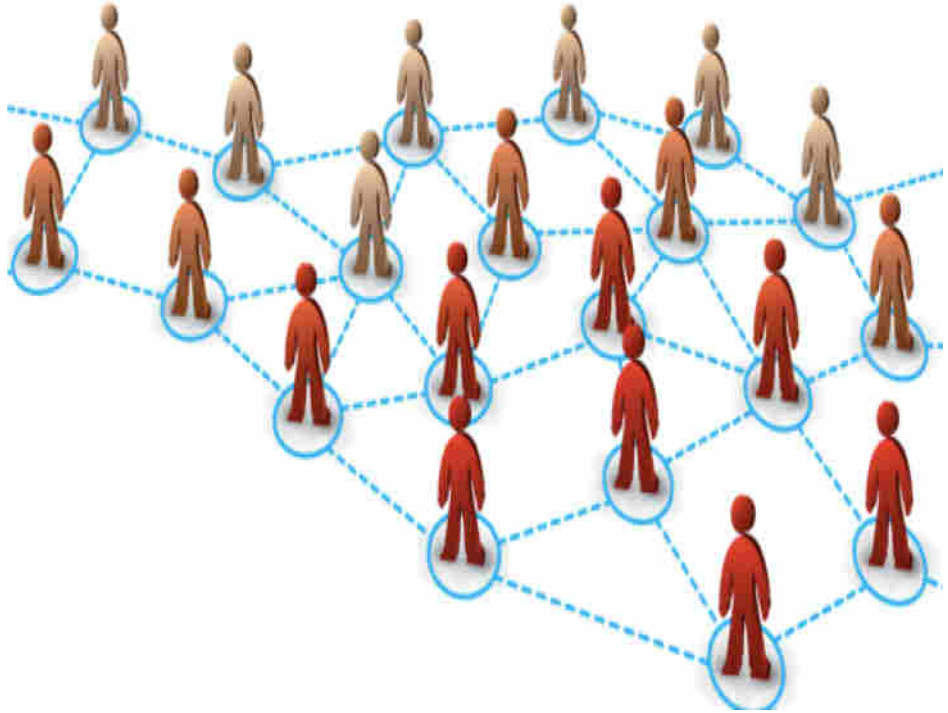
Tuttavia, tali organizzazioni devono conservare solo registrazioni delle attività di trattamento per i tipi di trattamento menzionati dall'articolo 30, paragrafo 5….

Attribuzione di compiti e funzioni all'interno dell'organizzazione

Training of Trainers

RGPD Art. 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (C81)

1. Il responsabile del trattamento, o **chiunque agisca sotto la sua autorità** o sotto quella del titolare del trattamento, che abbia accesso a dati personali **non può trattare 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.



Codice Privacy - Art. 2-*quaterdecies (Attribuzione di funzioni e compiti a soggetti designati)*

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e **nell'ambito del proprio assetto organizzativo**, che **specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche**, espressamente designate, che operano sotto la loro autorità.

la matrice RACI: ruoli e responsabilità

Training of Trainers

Referente dell'attività: soggetto che, nella pratica quotidiana, è responsabile delle attività di trattamento: il "*proprietario*" del trattamento

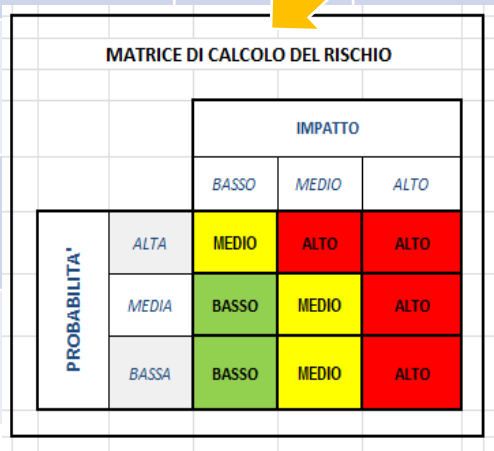
	Responsible	Accountable	Consulted	Informed
Top Management		X		
Referente	X			
RPD			X	
Dipartimento IT			X	
Responsabili, se del caso			X	

Responsible	Ha l'obbligo di azione e di decisione per il raggiungimento dei risultati richiesti
Accountable	Risponde delle azioni, delle decisioni e della prestazione
Consulted	Contribuisce e fornisce commenti
Informed	Viene tenuto informato delle decisioni prese e del trattamento

Fonte: European Data Protection Supervisor -Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, febbraio 2018, p. 4

ESERCIZIO
REGISTRO – ESEMPIO Di RACCOLTA DATI E VALUTAZIONE

Training of Trainers

1. ACQUISIZIONE DATI
2. VERIFICA CONFORMITA’

	NOME ATTIVITÀ DI TRATTAMENTO	NOME DEL DIPARTIMENTO COMPETENTE /OWNER DEI DATI	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	FINALITA’	BASI LEGALI	TEMPI DI COSERVAZIONE	ATTIVITA DI TRATTAMENTO ESEGUITE	RESPONSABILI DEL TRATTAMENTO	SOGGETTI A CUI VENGONO COMUNICATI I DATI	TRASFERIMENTI A PAESI – ORAGANIZ. INTERNAZIONALI	SISTEMI ICT COINVOLTI (INTERNI –ESTERNI)	LIVELLO DI RISCHIO	MISURE DI SICUREZZA ADOTTATE
1														
2														
…														
n