Requisiti di Conformità e di Accountability di un modello organizzativo Privacy

Privacy e Dlgs 231/2001

Federprivacy - Seminario online- Venerdì 14 maggio 2021

Luigi Carrozzi

Funzionario direttivo presso il Garante per la protezione dei dati personali

Il contento di questa presentazione è reso a livello personale e non impegna l'ente di appartenenza

Agenda

- Premessa: obiettivo del GDPR
- Principio di Accountability
- Modello organizzativo privacy: conformità
- Modello organizzativo privacy: accountability
- Organizzazione privacy: conformità e accountability sul «campo»

Il modello organizzativo privacy

Requisiti di conformità e di accountability del modello organizzativo Privacy

Faremo riferimento

- ai principi generali e alle disposizioni del Regolamento e del Codice di cui dobbiamo tenere conto nel costruire il nostro modello

- ad alcune «buone pratiche» per costruire un modello organizzativo privacy «robusto» che possa supportare il titolare nel raggiungimento del suo obiettivo di «accountability»

CONFORMITÀ	ACCOUNTABILITY
Caratteristiche di conformità del modello organizzativo alle disposizioni del GDPR	Caratteristiche di un modello organizzativo tali che possano identificare il titolare del trattamento come "Accountable" secondo il GDPR

Premessa: obiettivo del GDPR

GDPR: Il valore da proteggere

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)

Articolo 1 - **Oggetto e finalità**

Paragrafo 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.**

Correnti sfide della protezione dei dati personali

GDPR – Considerando 6

- livello di utilizzo di dati personali senza precedenti;
- portata della condivisione e della raccolta di dati personali;
- globalizzazione;
- rapidità dell'evoluzione tecnologica;
- le informazioni personali sono rese pubbliche su scala globale dagli interessati

I rischi per le persone fisiche

RGPD Considerando (75)

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare **da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale**, in particolare: se il trattamento può comportare

- **discriminazioni,**
- **furto o usurpazione d'identità,**
- **perdite finanziarie,**
- **pregiudizio alla reputazione,**
- **perdita di riservatezza dei dati personali protetti da segreto professionale**
- **decifratura non autorizzata della pseudonimizzazione**
- **Rischio per gli interessati:**
  - **di essere privati dei loro diritti e delle loro libertà**
  - **venga loro impedito l'esercizio del controllo sui dati personali che li riguardano**
- **qualsiasi altro danno economico o sociale significativo**

Valore da proteggere per la persona e per la società

The risk-based approach goes beyond a narrow "harm-based-approach" that concentrates only on damage ……on the person concerned by the processing in question,

to a general societal impact (e.g. loss of social trust)»

«Fonte: dichiarazione del 27 febbraio 2013 del WP 29 sulle discussioni in corso riguardanti il pacchetto di riforma della protezione dei dati - punti 8 e 11»

Il principio di Accountability

*"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)"*

Fonte: WP29 - WP243 - Linee guida sui responsabili della protezione dei dati

L'articolo 5 del GDPR sancisce i principi del trattamento dei dati personali

Il paragrafo 1 declina i principi fondamentali:

- *liceità,*
- *correttezza,*
- *trasparenza,*
- *limitazione delle finalità,*
- *minimizzazione dei dati,*
- *accuratezza,*
- *limitazione della conservazione,*
- *sicurezza*

Il paragrafo 2 stabilisce:

"The controller shall be ***responsible for,*** *and* ***be able to demonstrate*** *compliance with, paragraph 1 ('accountability')"*

Art. 24 Responsabilità del titolare del trattamento

Par. 1)

Tenuto conto

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

del trattamento, nonché

- dei **rischi** aventi **probabilità** e **gravità** diverse per i diritti e le libertà delle persone fisiche,

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 presente regolamento.

Art 24 Responsabilità del titolare del trattamento

Par. 2)

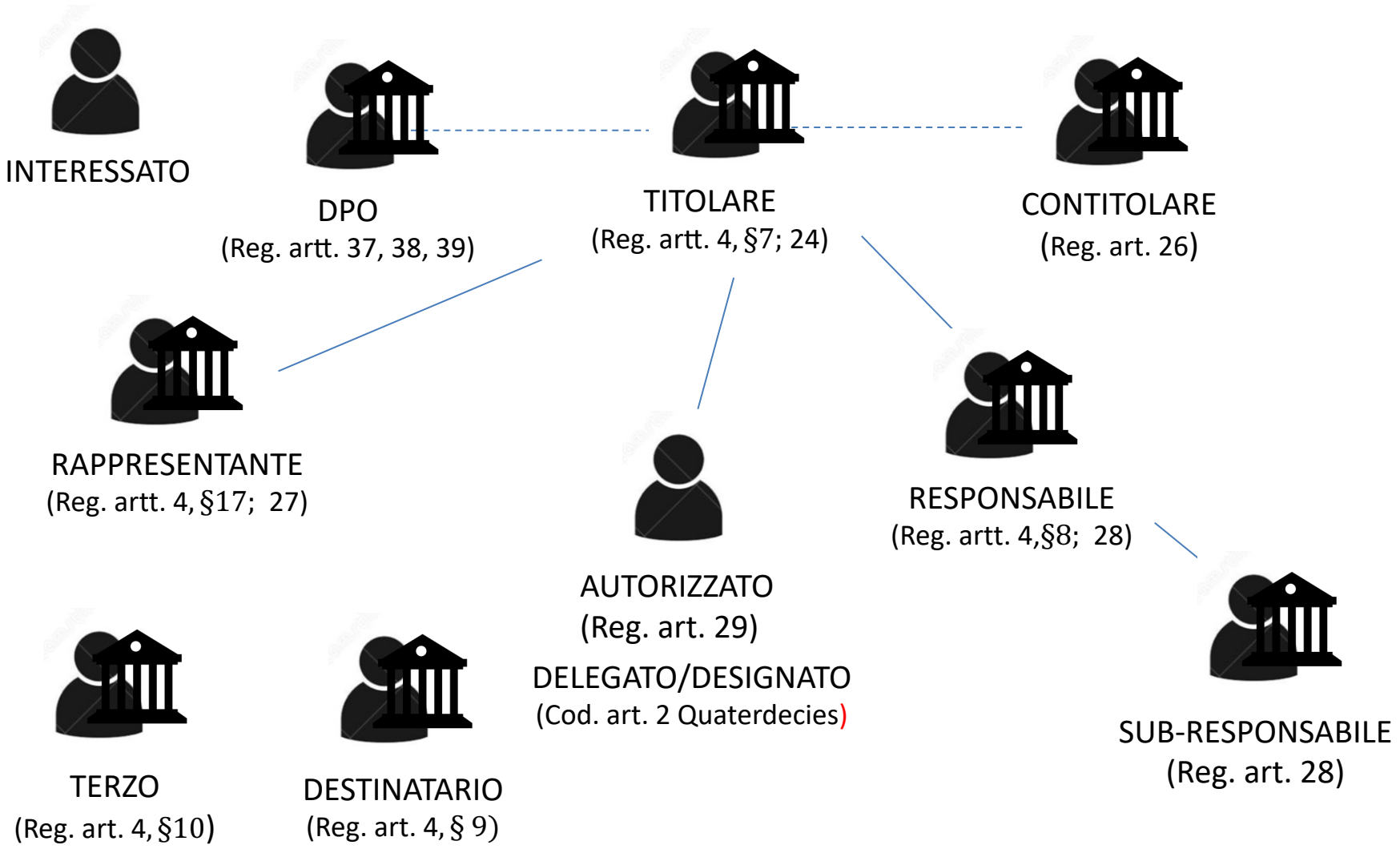
Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono **l'attuazione di politiche adeguate** in materia di protezione dei dati da parte del titolare del trattamento.

Par. 3)

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

Modello organizzativo privacy: conformità

Attori privacy secondo il Regolamento ed il Codice



*il Regolamento e il Codice prevedono **figure** con specifici **ruoli, relazioni tra i i ruoli** e **responsabilità** che, debbono agire nei casi e nei modi prescritti*

Modello organizzativo privacy: accountability

La necessità di una chiara ripartizione delle responsabilità tra gli attori privacy

CONSIDERANDO 79

- **La protezione dei diritti e delle libertà degli interessati** così come
- **la responsabilità generale (*responsibility + liability*) dei titolari del trattamento e dei responsabili del trattamento**,
- anche in relazione al **monitoraggio** e alle **misure delle autorità di controllo**,

esigono

- **una chiara ripartizione delle responsabilità** ai sensi del presente regolamento

compresi i casi in cui un **titolare** del trattamento stabilisca le finalità e i mezzi del trattamento **congiuntamente con altri titolari** del trattamento o quando **l'operazione di trattamento viene eseguita per conto del titolare** del trattamento.

Competenza degli attori

RESPONSABILE DEL TRATTAMENTO

Considerando 81

*…….Per garantire che siano rispettate le prescrizioni del presente regolamento ….**il titolare del trattamento** dovrebbe ricorrere unicamente a **responsabili del trattamento** **che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse**, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento….*

RESPONSABILE DELLA PROTEZIONE DEI DATI

WP29 - Linee-guida sui responsabili della protezione dei dati - Pag.12

*…….**E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare;** inoltre, il RPD dovrebbe avere buona familiarità con le **operazioni di trattamento svolte** nonché con **i sistemi informativi e le esigenze di sicurezza e protezione dati** manifestate dal titolare.*

*Nel caso di **un'autorità pubblica** o di un organismo pubblico, il RPD dovrebbe possedere anche una **conoscenza approfondita delle norme e procedure amministrative applicabili……***

La leva organizzativa: attribuzione di compiti e funzioni all'interno dell'organizzazione

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

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.

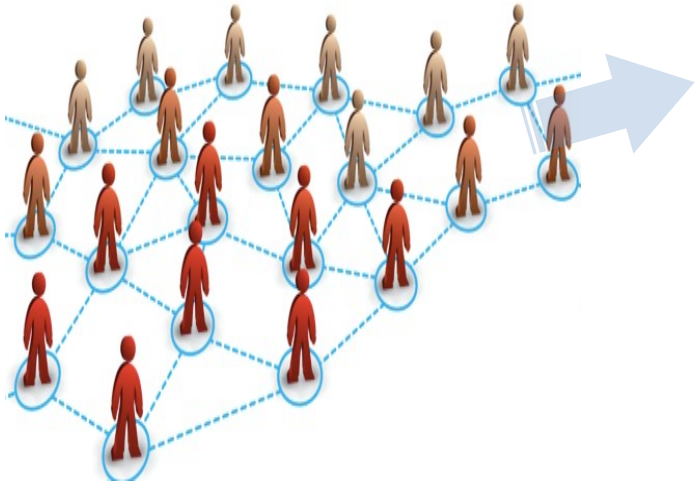
Codice Privacy - Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati*)*

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.

Organizzazione privacy: Conformità e Accountability sul «campo»

Organizzazione: Persone, Policy e Processi

- **Riconoscere e far conoscere l'obiettivo di valore da perseguire**
- **Rendere l'organizzazione capace di perseguire l'obiettivo in maniera sostanziale*:***
  - stabilire gli obiettivi e comunicarli a tutta l'organizzazione
  - assegnare ruoli e responsabilità
  - individuare le competenze necessarie
  - stabilire regole (policy), processi e procedure
  - identificare gli asset (dati, tecnologie, processi aziendali rilevanti privacy)
  - analisi dei rischi e individuazione/adeguamento misure tecniche e organizzative (miglioramento continuo)
  - ……



Fattori chiave di successo

- **integrare la protezione dei dati personali nella gestione dell'attività d'impresa**
- **perseguire la conformità al Regolamento ed al Codice in ottica «sostanziale»**

Presidiare le principali aree di processo privacy

Allocare all'interno dell'organizzazione **RUOLI E RESPONSABILITÀ** privacy	Identificare e **REGISTRARE LE ATTIVITÀ DI TRATTAMENTO** dei dati personali ed i relativi asset coinvolti	Effettuare **ANALISI DEI RISCHI su base** ricorrente e **valutazioni di impatto privacy** laddove previsto ;	Attuare adeguate **MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE** e rivederne su base continuativa l'adeguatezza;
Definire e far rispettare specifiche **POLICY di protezione dei dati**;	Identificare i **PROCESSI E LE PROCEDURE** che garantiscono **il rispetto dei principi del GDPR**	adottare l'approccio **PRIVACY BY DESIGN E BY DEFAULT**	Adesione a **CODICI DI CONDOTTA ed ottenere CERTIFICAZIONI**
Gestire le terze parti individuabili come **RESPONSALI DEL TRATTAMENTO**	Disporre di un processo finalizzato alla **GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI**;	Gestire le richieste di **ESERCIZIO DEI DIRITTI DA PARTE DEGLI INTERESSATI**	Effettuare attività **di FORMAZIONE E TRAINING** (su attività operative) **del personale**
Gestione eventuali **TRASFERIMENTI DATI ALL'ETERO**	Disporre di un sistema di **VALUTAZIONE DELL'EFFICACIA DELLE MISURE**		

Scalabilità dei dispositivi del GDPR e loro applicazione sostanziale

"The Working Party recognizes that some of the provisions in the proposed Regulation may pose a burden on some controllers which may be perceived as unbalanced and has therefore in earlier opinions already expressed the view ***that all obligations*** ***must be scalable to the controller and the processing operations concerned.***

Compliance should never be a box ticking exercise*, but should really be about ensuring that personal data is sufficiently protected. How this is done, may differ per controller…….* ***Data subjects should have the same level of protection, regardless of the size of the organisation or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a scalable manner."***

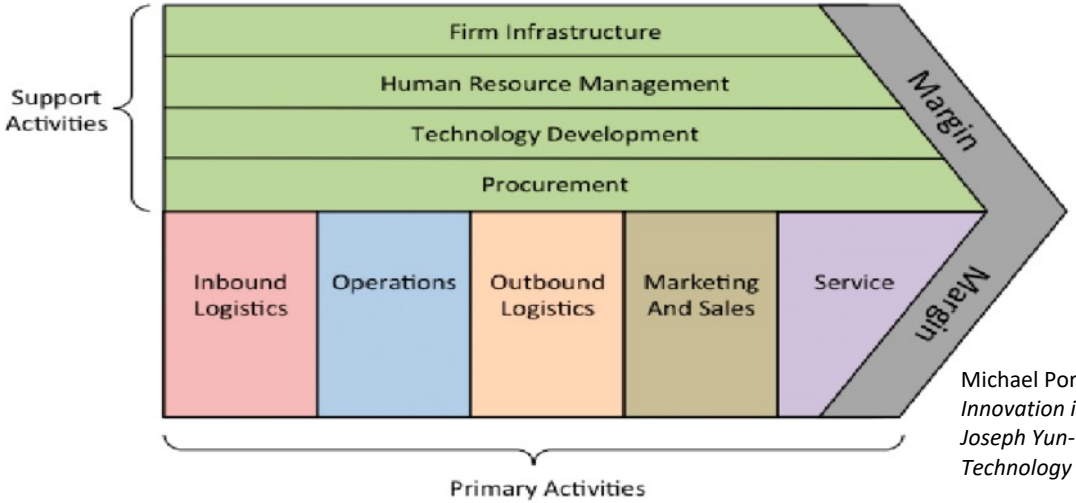
Fonte: Statement of the WP29 of 27 February 2013 on current discussions regarding the data protection reform package on the role of a risk-based approach in data protection legal frameworks.

Accountability e registro delle attività di trattamento

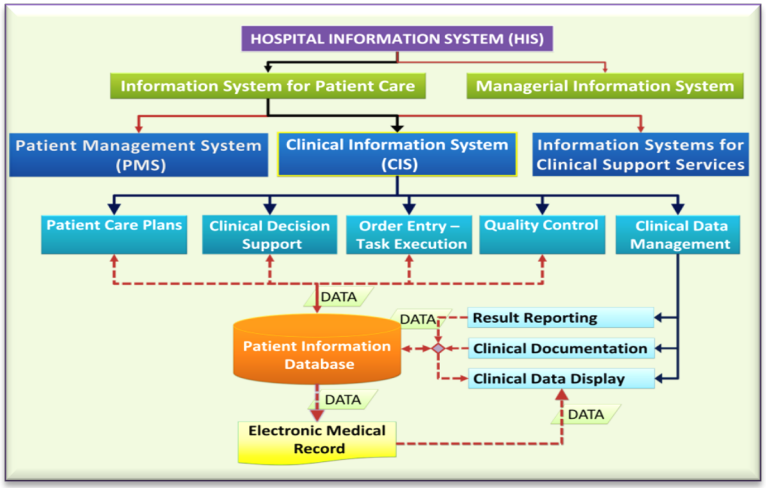
Rendere una entità Accountable significa assegnare compiti da eseguire e decisioni da assumere **e aspettarsi che tale entità risponda del suo operato e delle decisioni prese.**
In questo senso, l'accountability è **l'essere tenuti a rispondere** dei compiti assegnati delle decisioni che ci competono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

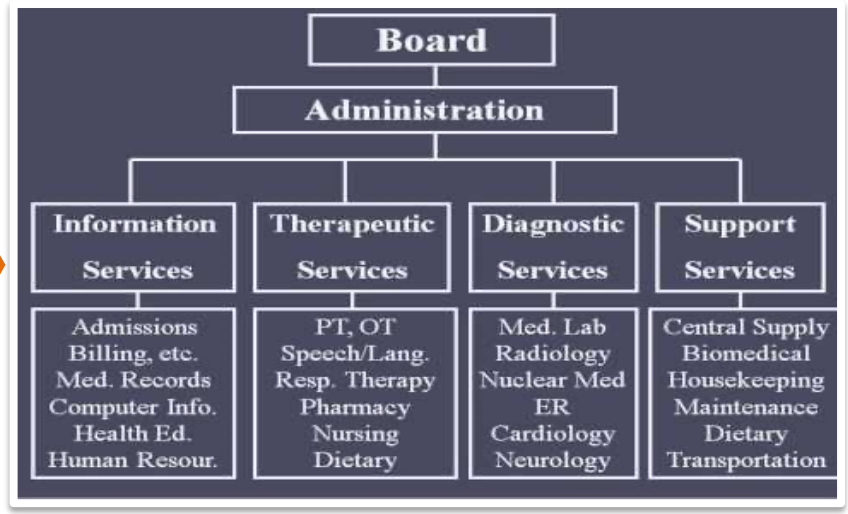
Conoscenza delle attività di trattamento all'interno dell'organizzazione e attribuzione di ruoli e responsabilità



Michael Porter's value chain: - Source: *Editorial Open Innovation in Value Chain for Sustainability of firms- Jinhyo Joseph Yun- Daegu Gyeongbuk Institute of Science and Technology*



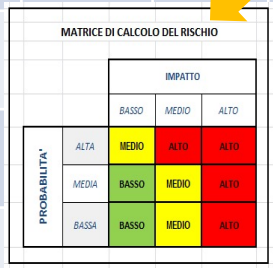
Functional Components of a Clinical Information System
Source: Dr. Abdollah Salleh - https://drdollah.com/clinical-information-system



Source: Principles of Health Science
https://www.youtube.com/watch?v=FpQEwbAV3Qw

Accountability - esempio di registro delle attivita' di trattamento e modello organizzativo

	NOME ATTIVITÀ DI TRATTAMENTO	NOME DEL DIPARTIMENTO COMPETENTE /OWNER ATTIVITA'	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														



LA MATRICE RACI: RUOLI E RESPONSABILITÀ

Delegato/Designato privacy - Referente dell'attività: soggetto che, nella pratica quotidiana, è «responsabile» delle attività di trattamento: in qualità di "*owner*" del processo che prevede quella attività di 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

Efficacia dell'azione del titolare

Considerando (74)

…..In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto ***misure adeguate ed efficaci*** ***ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure…..***

Performance del modello organizzativo

PRINCIPALI AREE DI PROCESSO PRIVACY

1. Ruoli e responsabilità
2. Policy di protezione dei dati
3. Attività di trattamento dei dati personali
4. Rispetto dei principi del GDPR
5. Valutazione del rischio e DPIA
6. Privacy by design e by default
7. Responsali del trattamento
8. Esercizio dei diritti degli interessati
9. Trasferimento dati all'estero
10. Misure di sicurezza
11. Violazioni dei dati personali
12. Codici di condotta e certificazioni
13. Formazione e training
14. Valutazione efficacia framework privacy

LIVELLO DI MATURITÀ

Fonte dell'iimagine: The Process Group - CMMI V2.0