GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

Cofinanziato dall'Unione Europea

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Luigi Carrozzi

Funzionario direttivo presso il Garante per la protezione dei dati personali

AGENDA

- **INTRODUZIONE**
- IL REGISTRO ED IL **PRINCIPIO DI ACCOUNTABILTY**
- **STRUTTURA DEL REGISTRO** E PREVISIONI REGOLAMENTARI
- **CONTENUTO DEL REGISTRO - ESEMPIO**
- POSSIBILI **ULTERIORI INFORMAZIONI** DA INSERIRE NEL REGISTRO
- **APPROCCIO ORGANIZZATIVO** ALLA COSTITUZIONE DEL REGISTRO
- **REGISTRO** E **RESPONSABILE DELLA PROTEZIONE DATI**

INTRODUZIONE

IL REGOLAMENTO

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)

OBIETTIVI DEL TRATTAMENTO DEI DATI PERSONALI

RGPD - CONSIDERANDO 4)

«Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo»…

TECNOLOGIA E CONTESTO

RGPD - CONSIDERANDO 6

- ***La rapidità*** *dell'evoluzione* ***tecnologica*** *e la globalizzazione comportano nuove sfide per la protezione dei dati personali.*
- *La* ***portata della condivisione*** *e della* ***raccolta*** *di dati personali è aumentata in modo significativo.*
- *La tecnologia attuale consente tanto alle i****mprese private*** *quanto alle* ***autorità pubbliche*** *di* ***utilizzare dati personali, come mai in precedenza,*** *nello svolgimento delle loro attività.*

- *Sempre più spesso, le persone fisiche* ***rendono disponibili al pubblico su scala mondiale informazioni personali*** *che li riguardano.*

RGPD - CONSIDERANDO 6

La tecnologia ha trasformato l'economia e le relazioni sociali

- ***dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione*** *e il loro trasferimento verso paesi terzi e organizzazioni internazionali,*
- ***garantendo al tempo stesso un elevato livello di protezione dei dati personali****.*

RGPD - CONSIDERANDO 7

- *Tale evoluzione richiede un **quadro più solido** e coerente in materia di protezione dei dati nell'Unione, **affiancato da efficaci misure di attuazione,** data l'importanza di **creare il clima di fiducia** che **consentirà lo sviluppo dell'economia digitale in tutto il mercato interno.***
- *È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le **persone fisiche** quanto per gli **operatori economici** e le **autorità pubbliche**.*

OBIETTIVI DEL REGISTRO

1)Supportare il titolare ad agire in conformità ai principi ed alle disposizioni del regolamento

2) Supportare Il Garante nelle attività di sorveglianza sull'applicazione del Regolamento

IL REGISTRO ED IL PRINCIPIO DI ACCOUNTABILTY

ACCOUNTABILITY E RGPD

"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 - Gruppo di lavoro sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali – (WP243 - Linee guida sui responsabili della protezione dei dati)

RGPD - PRINCIPI

RGPD Art. 5)

Il paragrafo 1) prevede i principi fondamentali del trattamento dei dati personali:

- **liceità, correttezza** e **trasparenza**
- **limitazione delle finalità**
- **minimizzazione dei dati**
- **esattezza**
- **limitazione della conservazione**
- **sicurezza** (integrità e riservatezza).

Il paragrafo 2) stabilisce:

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

RGPD- Responsabilità del titolare

Articolo 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.*

Dette misure sono riesaminate e aggiornate qualora necessario

NATURA, AMBITO DI APPLICAZIONE, CONTESTO E FINALITÀ DEL TRATTAMENTO

EDPB - Linee guida sull'articolo 25 - Versione 2.0 (par. 2.1.3.2)

*«Il RGPD **adotta un approccio coerente basato sul rischio** in molte delle sue disposizioni, **negli articoli 24, 25, 32 e 35**, al fine di individuare le misure tecniche e organizzative adeguate per tutelare le persone fisiche e i loro dati personali nonché adempiere ai requisiti del RGPD. **I beni da tutelare sono sempre gli stessi (le persone fisiche, mediante la protezione dei loro dati personali),** identici sono i rischi (per i diritti delle persone fisiche), e identiche le condizioni di cui tenere conto (**natura**, **ambito di applicazione**, **contesto** e **finalità del trattamento**).»*

NATURA, AMBITO DI APPLICAZIONE, CONTESTO E FINALITÀ DEL TRATTAMENTO

EDPB - Linee guida sull'articolo 25 - Versione 2.0 (par. 2.1.3.3)

I titolari devono tenere conto della **natura, dell'ambito di applicazione, del contesto e della finalità del trattamento** allorché determinano le misure necessarie.

Questi fattori devono essere interpretati in modo coerente con il ruolo ad essi attribuito in altre disposizioni del RGPD, quali **gli articoli 24, 32 e 35,** allo scopo di integrare principi di protezione dei dati nella progettazione del trattamento.

In breve, il concetto di

- **natura** può essere inteso come le **caratteristiche intrinseche** (*) **del trattamento**
- **l'ambito di applicazione** (n.d.r. ***scope***), fa riferimento **alla dimensione e all'ampiezza del trattamento**
- **Il contesto** riguarda le **circostanze nel trattamento che possono influenzare le aspettative degli interessati**, mentre
- la **finalità** si riferisce agli **obiettivi del trattamento**.

(*) *Ne sono esempi le categorie particolari di dati personali, il processo decisionale automatizzato, i rapporti di forza asimmetrici, l'imprevedibilità del trattamento, la difficoltà per l'interessato di esercitare i propri diritti, ecc.*

IMPORTANZA DEL REGISTRO

Il Registro consente in particolare di:

- possedere una **completa ricognizione e valutazione delle attività di trattamento**
- raccogliere elementi fondamentali ai fini delle **analisi del rischio delle attività di trattamento** e la conseguente individuazione delle **misure di sicurezza** da adottare

E' strumento idoneo a garantireun adeguato e continuo rispetto del RGPD nelle organizzazioni.

Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione.

Il Registro si configura inoltre come strumento di **cooperazione tra titolari e Autorità di Controllo** e per agevolare le **attività di sorveglianza** di queste ultime.

ACCOUNTABILITY E REGISTRO (I)

In termini generali rendere un soggetto *Accountable* significa **assegnare responsabilità e compiti**, che comportano presa di decisioni e attività da svolgere, e **aspettarsi che tale soggetto risponda delle decisioni prese e del suo operato.**

Nel RGPD per *Accountability* si **intende che il titolare del trattamento ha la responsabilità di garantire la conformità al Regolamento e che è in grado di dimostrare tale conformità**

ACCOUNTABILITY E REGISTRO (II)

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 controllare detti trattamenti.***

ACCOUNTABILITY E REGISTRO (III)

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 supporta, tra l'altro, la valutazione del rischio sui diritti e le libertà delle persone e l'identificazione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

STRUTTURA DEL REGISTRO E PREVISIONI REGOLAMENTARI

ARTICOLO 30 - REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO (Par. 1- TITOLARI)

1. **Ogni titolare del trattamento** e, ove applicabile, il suo rappresentante tengono **(*)** un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il **nome e i dati di contatto del titolare** del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le **finalità del trattamento**;

c) una descrizione delle **categorie di interessati** e delle **categorie di dati personali**;

d) **le categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di **paesi terzi od organizzazioni internazionali**;

e) ove applicabile, **i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale**, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 (par. 1) (**), la documentazione delle garanzie adeguate;

f) ove possibile**, i termini ultimi previsti per la cancellazione** delle diverse categorie di dati;

g) ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1.

(*) Nel testo inglese «***shall maintain***»

(**) Cfr.: Art 49, par. 6

REGISTRO DEI TRATTAMENTI – TITOLARE

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**

Modello di "registro semplificato" delle attività di trattamento del titolare per PMI
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048342

ARTICOLO 30 - REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO (Par. 2 - RESPONSABILI)

Ogni responsabile del trattamento (e, ove applicabile, il suo rappresentante) tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) **il nome e i dati di contatto del responsabile** o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) **le categorie dei trattamenti** effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, **i trasferimenti di dati personali verso un paese terzo** o **un'organizzazione internazionale**, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 (par. 1) (*), la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle **misure di sicurezza** tecniche e organizzative di cui all'articolo 32, paragrafo 1.

(*) Cfr.: Art 49, par. 6

REGISTRO DEI TRATTAMENTI – RESPONSABILE (art. 30.2)

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**

Modello di "registro semplificato" delle attività di trattamento del responsabile per PMI
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048348

REGISTRO DEI TRATTAMENTI – RESPONSABILE

Il responsabile del trattamento tiene un registro di "tutte le categorie di attività relative al trattamento svolte per conto di un titolare" (art. 30, par. 2 del RGPD).

- Nel caso in cui **uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari** (es. società di software house) le informazioni di cui all'art. 30, par. 2 del RGPD **dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari**.
- In questi casi il **responsabile dovrà suddividere il registro in tante sezioni quanti sono i titolari per conto dei quali agisce.**
- *Ove, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento*
  - *dei nominativi degli stessi, nonché*
  - *di correlazione delle categorie di trattamenti svolti per ognuno di essi,*

risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ***ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, par. 2 del RGPD;***

Cfr.: Garante Privacy - FAQ sul registro delle attività di trattamento
https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

REGISTRO DEI TRATTAMENTI – RESPONSABILE

- con riferimento alla "descrizione delle categorie di trattamenti effettuati" è **possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell'art. 28 del RGPD**, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo;

- in caso **di sub-responsabile**, parimenti, il registro delle attività di trattamento svolte da quest'ultimo **potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi** dell'art. 28, paragrafi 2 e 4 del RGPD.

Cfr.: FAQ sul registro delle attività di trattamento
https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

BUONE PRATICHE PER LA COMPILAZIONE DEL REGISTRO

1. Inserire tutte le informazioni relative ai temi delle indicati dalle **disposizioni di cui all'art. 30 RGPD,** adottando il ad es. il modello predisposto dal Garante, in maniera adeguata alla realtà del trattamento e facilmente comprensibile.
2. Specificare per ciascun tema **tutte le necessarie informazioni che caratterizzano il trattamento** soprattutto quando tali informazioni sono correlate a (in quanto implicano) specifici adempimenti previsti dal RGPD (es.: necessità di DPIA).
3. Inserire tutte le **ulteriori informazioni ritenute opportune per rendere il registro uno strumento «operativo»** che consente, per quanto possibile, al titolare/responsabile di avere adeguata consapevolezza dei trattamenti che avvengono sotto la sua responsabilità e di tutte le attività che deve necessariamente effettuare per garantire la conformità al RGPD

REGISTRO DEI TRATTAMENTI – FORMA SCRITTA; AUTORITA' DI CONTROLLO (art. 30.3 e 30.4)

30.3
I registri di cui ai paragrafi 1 e 2 sono tenuti in **forma scritta**, anche in formato elettronico

30.4
Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento **mettono il registro a disposizione dell'autorità di controllo**.

TENUTA DEL REGISTRO DEI TRATTAMENTI - DEROGA PER LE PICCOLE E MEDIE IMPRESE (art. 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….

REGISTRO: LE FAQ DEL GARANTE

Il Garante per la protezione dei dati personali con un comunicato stampa dell'8 ottobre 2018 ha messo a disposizione delle "FAQ sul registro delle attività di trattamento":
https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

Le FAQ del Garante contengono una serie di ulteriori precisazioni:

- sulla categoria delle "organizzazioni" di cui all'art. 30, par. 5, rientrandovi anche le **associazioni, le fondazioni e i comitati**;
- sui soggetti tenuti all'obbligo di redazione del registro come, ad esempio:
  - **esercizi commerciali, esercizi pubblici o artigiani** con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, etc.) e/o **che trattino dati sanitari dei clienti** (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori etc.);
  - **liberi professionisti** con almeno un dipendente **e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati** (es. commercialisti, avvocati, notai, farmacisti, medici in generale etc.)
  - **associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penale o reati** (i.e. organizzazioni di tendenza, associazioni a tutela di soggetti c.d "vulnerabili", associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni; associazioni sportive con riferimento ai dati sanitari etc.)
  - **il condominio ove tratti "categorie particolari di dati"**(es. delibere per interventi volti al superamento di barriere architettoniche etc.)

30

REGISTRO: FAQ DEL GARANTE - RACCOMANDAZIONI

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del RGPD, ***il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento****, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti,* ***contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability*** *e, al contempo, ad* ***agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.***

FAQ sul registro delle attività di trattamento

https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

CONTENUTO DEL REGISTRO - ESEMPIO

DATA DI COMPILAZIONE E AGGIORNAMENTO

Il Registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento.

Date

- La data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento)
- La data dell'ultimo aggiornamento

Esempio:

- Data istituzione/Scheda creata in data __.__._____
- Ultimo aggiornamento avvenuto in data __.__._____

NOME E DATI DI CONTATTO DEL TITOLARE

a) il nome e i dati di contatto del **titolare** del trattamento e, ove applicabile, del **contitolare** del trattamento, del **rappresentante del titolare** del trattamento e del **responsabile della protezione** dei dati;

Nome e dati di contatto di
• Titolare • (Contitolare) • (Rappresentante del Titolare) • (Responsabile della protezione dati)
Esempio: *Nome, Indirizzo, Email, Telefono…*

TIPOLOGIA

Identificare il trattamento attraverso una descrizione della tipologia dell'attività svolta

TIPOLOGIA DI TRATTAMENTO
Esempio: •Risorse Umane – Trattamenti nell'ambito della **Gestione del Personale** •Marketing e Vendite – Trattamenti nell'ambito della **Gestione delle Vendite** •Approvvigionamenti – Trattamenti nell'ambito della **Gestione Magazzino**

FINALITA' DEL TRATTAMENTO

b) le finalità del trattamento;

Finalità del trattamento

Esempio:

- **Gestione del rapporto di lavoro**
- **Gestione della clientela**
- **Gestione dei fornitori**

BASI LEGALI DEL TRATTAMENTO

Basi legali del Trattamento

Esempio:

- Consenso
- Esecuzione di un contratto
- Obbligo legale
- ……..
- legittimo interesse concretamente perseguito con:
  - eventuali «garanzie adeguate» approntate,
  - eventuale «preventiva valutazione d'impatto» posta in essere dal titolare (*cfr. Garante: Doc-Web n. 8080493*)

CATEGORIE DI INTERESSATI

c) una descrizione delle **categorie di interessati** …

Categorie di interessati
Esempio: • Dipendenti e candidati nei processi di selezione del personale • Clienti • Fornitori

CATEGORIE DI INTERESSATI E DI DATI PERSONALI

c) …….e delle **categorie di dati personali**;

Categorie di dati personali
Esempio: • dati anagrafici • dati sanitari • dati biometrici • dati genetici • dati relativi a condanne penali o reati

- In caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'art. 9, par. 2, a) - j) del RGPD;

- In caso di trattamenti di " dati relativi a condanne penali e reati ", riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del RGPD

DESTINATARI

(d) **le categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

Atri titolari o responsabili cui saranno comunicati i dati

Esempio:

- altri titolari pubblici (es. enti previdenziali per gestione contributi dei dipendenti)
- eventuali responsabili e sub-responsabili del trattamento (es. fornitore esterno per servizio di elaborazione buste paga dei dipendenti)

TRASFERIMENTI VERSO PAESI ESTERI

(e) ove applicabile, **i trasferimenti di dati personali verso un paese terzo** o **un'organizzazione internazionale**, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, par. 1, **la documentazione delle garanzie adeguate;**

Trasferimenti e Paese/Organizzazione Internazionale

Inserire:

- Informazioni sui trasferimenti di dati personali
- I Paesi terzi cui i dati sono trasferiti
- Le "garanzie" adottate ai sensi del capo V del RGPD (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.), compreso quanto disposto dall'art. 49 par. 6.

TERMINI ULTIMI DI CANCELLAZIONE

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

Tempi di cancellazione per tipologia e finalità di trattamento

- Indicare i tempi di cancellazione per tipologia e finalità di trattamento (ad es. “in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall’ultima registrazione – v. art. 2220 del codice civile”) e comunque conformemente ai principio di limitazione della conservazione
- Ove **non sia possibile stabilire a priori un termine massimo**, **fare riferimento ai criteri adottati**. Indicare eventuali norme di legge di riferimento (es. norme di legge, prassi settoriali) indicativi degli stessi (es. “in caso di contenzioso, i dati saranno cancellati al termine dello stesso”.

MISURE DI SICUREZZA

(g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Misure di sicurezza tecniche ed organizzative

- Vanno indicate le **misure tecnico-organizzative** adottate dal titolare ai sensi dell'art. 32 del RGDP
- **L'individuazione è rimessa al titolare** in relazione al livello di sicurezza ritenuto adeguato tenuto conto dei rischi presentati dalle attività di trattamento concretamente poste in essere.
- **Tale lista ha di per sé un carattere dinamico** in quanto dovrà tenere coto e continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi.
- Possono essere **descritte in forma riassuntiva** rinviando a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

POSSIBILI ULTERIORI INFORMAZIONI DA INSERIRE NEL REGISTRO

*«Può essere riportata nel registro qualsiasi altra informazione che il titolare o il responsabile ritengano utile indicare (ad es. le **modalità di raccolta del consenso**, le eventuali **valutazioni di impatto** effettuate, l'indicazione di eventuali "**referenti interni**" individuati dal titolare in merito ad alcune tipologie di trattamento ecc.)»*

Cfr.: Garante Privacy - FAQ sul registro delle attività di trattamento

MISURE DI SICUREZZA (I)

RGPD Articolo 32) - Sicurezza del trattamento

1. Tenendo conto:

- **dello stato dell'arte e dei costi di attuazione**,

nonché

- **della natura, dell'oggetto** («*scope*»), **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,….**

RGPD Articolo 32) - Sicurezza del trattamento (cont.)

…..che comprendono, tra le altre, se del caso:

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

b) la capacità di assicurare su base permanente la r**iservatezza, 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 personal**i 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.

CARATTERISTICHE DEI TRATTAMENTI + MISURE DI SICUREZZA

(Article 30 par. 1(a))	
	(*) *If applicable*
	CONTROLLER CONTACT DETAILS: Name, Address, Email, Telephone
	JOINT CONTROLLER CONTACT DETAILS (*) Name, Address, Email, Telephone
	REPRESENTATIVE CONTACT DETAILS (*) Name, Address, Email, Telephone
	DATA PROTECTION OFFICER CONTACT DETAIL (*) Name, Address, Email, Telephone

	(Article 30 par. 1(b)) PURPOSES OF THE PROCESSING	(Article 30 par. 1(c)) CATEGORIES OF DATA SUBJECTS	(Article 30 par. 1(c)) CATEGORIES OF PERSONAL DATA	(Article 30 par. 1(d)) CATEGORIES OF RECIPIENTS	(*) (Article 30 par 1(e)) TRANSFERS OF PERSONAL DATA TO A THIRD COUNTRY OR AN INTERNATIONAL ORGANISATION	(Article 30 par. 1(f)) TIME LIMITS FOR ERASURE		(Article 30 par. 1(g) TECHNICAL AND ORGANIZATIONAL MEASURES
1								
2								
3								
4								

RGPD - VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE DERIVANTI DAL TRATTAMENTI DI DATI PERSONALI

Un ***"rischio"*** è uno scenario che **descrive un evento** e le sue conseguenze, stimato in termini di **gravità e probabilità.**

La ***"gestione dei rischi»*** può essere definita come **l'insieme delle attività coordinate** volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

Fonte: WP 248 rev.01

RGPD – ANALISI DEI RISCHI - VALUTAZIONE DELLA PROBABLITA' E DELLA GRAVITA'

RGPD Considerando (83)

……

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**

RGPD - VALUTAZIONE DEI RISCHI

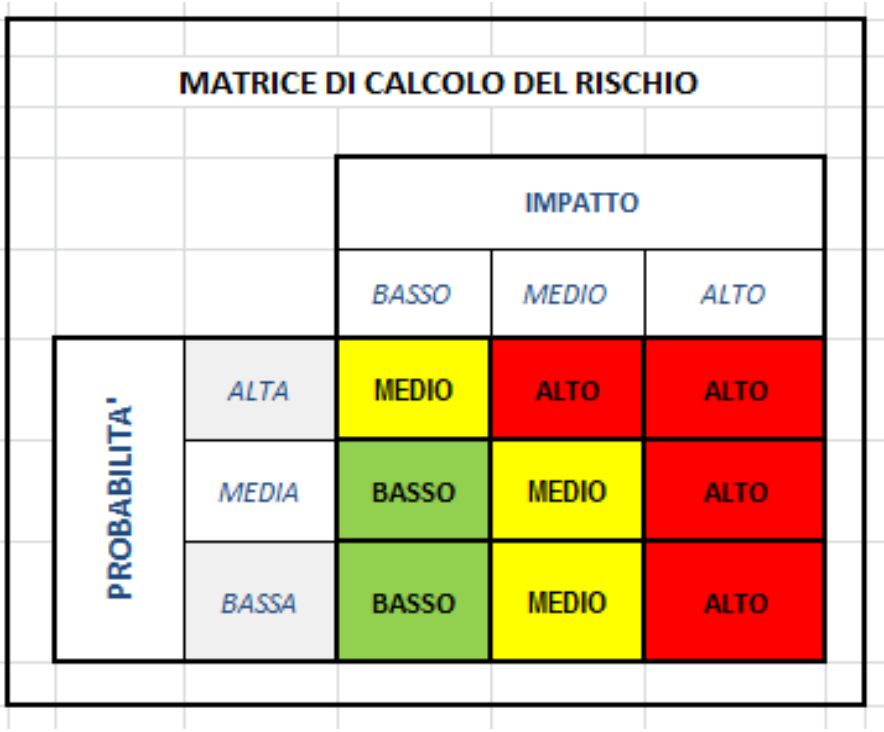
RGPD Considerando (75)

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, o**
- **qualsiasi altro danno economico o sociale significativo;**
- **se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o**
- **venga loro impedito l'esercizio del controllo sui dati personali che li riguardano.**

CALCOLO DEL RISCHIO

Per ciascuna minaccia può essere calcolato il corrispondente livello di rischio sulla base delle valutazioni di probabilità ed impatto entrambe espresse ad esempio su tre livelli di intensità : **ALTO – MEDIO – BASSO**



CARATTERISTICHE DEI TRATTAMENTI + MISURE DI SICUREZZA

(Article 30 par. 1(a))	
	(*) *If applicable*
	CONTROLLER CONTACT DETAILS: Name, Address, Email, Telephone
	JOINT CONTROLLER CONTACT DETAILS (*) Name, Address, Email, Telephone
	REPRESENTATIVE CONTACT DETAILS (*) Name, Address, Email, Telephone
	DATA PROTECTION OFFICER CONTACT DETAIL (*) Name, Address, Email, Telephone

	(Article 30 par. 1(b)) PURPOSES OF THE PROCESSING	(Article 30 par. 1(c)) CATEGORIES OF DATA SUBJECTS	(Article 30 par. 1(c)) CATEGORIES OF PERSONAL DATA	(Article 30 par. 1(d)) CATEGORIES OF RECIPIENTS	(*) (Article 30 par 1(e)) TRANSFERS OF PERSONAL DATA TO A THIRD COUNTRY OR AN INTERNATIONAL ORGANISATION	(Article 30 par. 1(f)) TIME LIMITS FOR ERASURE		(Article 30 par. 1(g) TECHNICAL AND ORGANIZATIONAL MEASURES
1								
2								
3								
4								

«DESCRIZIONE DEI TRATTAMENTI»

MISURE DI SICUREZZA

ULTERIORI INFORMAZIONI

DESCRIZIONE DEL TRATTAMENTO

RISK MANAGEMENT								
VIOLATION OF INTEGRITY			VIOLATION OF AVAILABILITY			VIOLATION OF CONFIDENTIALITY		
THREAT LIKELYHOOD (LOW, HIGH MEDIUM)	IMPACT (LOW, HIGH, MEDIUM)	RISK LEVEL (LOW, HIGH, MEDIUM)	THREAT LIKELYHOOD (LOW, HIGH MEDIUM)	IMPACT (LOW, HIGH, MEDIUM)	RISK LEVEL (LOW, HIGH, MEDIUM)	THREAT LIKELYHOOD (LOW, HIGH MEDIUM)	IMPACT (LOW, HIGH, MEDIUM)	RISK LEVEL (LOW, HIGH, MEDIUM)

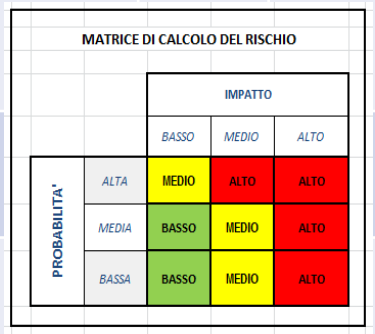
MISURE DI SICUREZZA

RISK		IMPACT		
		LOW	MEDIUM	HIGH
LIKELYHOOD	HIGH	MEDIUM	HIGH	HIGH
	MEDIUM	LOW	MEDIUM	HIGH
	LOW	LOW	MEDIUM	HIGH

POSSIBILI ULTERIORI INFORMAZIONI

Il registro come «***tableau de bord***» **per la conformità al RGPD** attraverso la **rilevazione** ed il **controllo** delle attività di trattamento

	NOME ATTIVITÀ DI TRATTAMENTO	NOME DEL DIPARTIMENTO COMPETENTE /REFERENTE INTERNO	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														



POSSIBLI ULTERIORI INFORMAZIONI

- Indicare la **funzione/servizio dell'organizzazione** responsabile delle attività di trattamento
- Specificare le **operazioni di trattamento** svolte sui dati (art. 4.2)
- Specificare se i dati sono archiviati su **supporti cartacei o elettronici**
- Specificare le **applicazioni utilizzate** per trattare i dati personali (es: strumenti di produttività individuale, applicazioni centralizzate, altri servizi applicativi, ecc.)
- Specificare le **tecnologie di memorizzazione e dove vengono archiviati i dati** (es: cloud, file server di rete locale, desktop, supporti rimovibili, ecc.)
- Specificare **strumenti e tecnologie di trasmissione** (es: email, FTP, altro)
- Tracciare le risultanze del processo di **analisi dei rischi**
- Indicare se le attività di trattamento sono soggette a **DPIA** ed in caso affermativo fare brevemente riferimento alla documentazione prodotta

APPROCCIO ORGANIZZATIVO ALLA COSTITUZIONE DEL REGISTRO

OWNERS, *ASSETS* ED IL PROCESSO DI GESTIONE DEI RISCHI

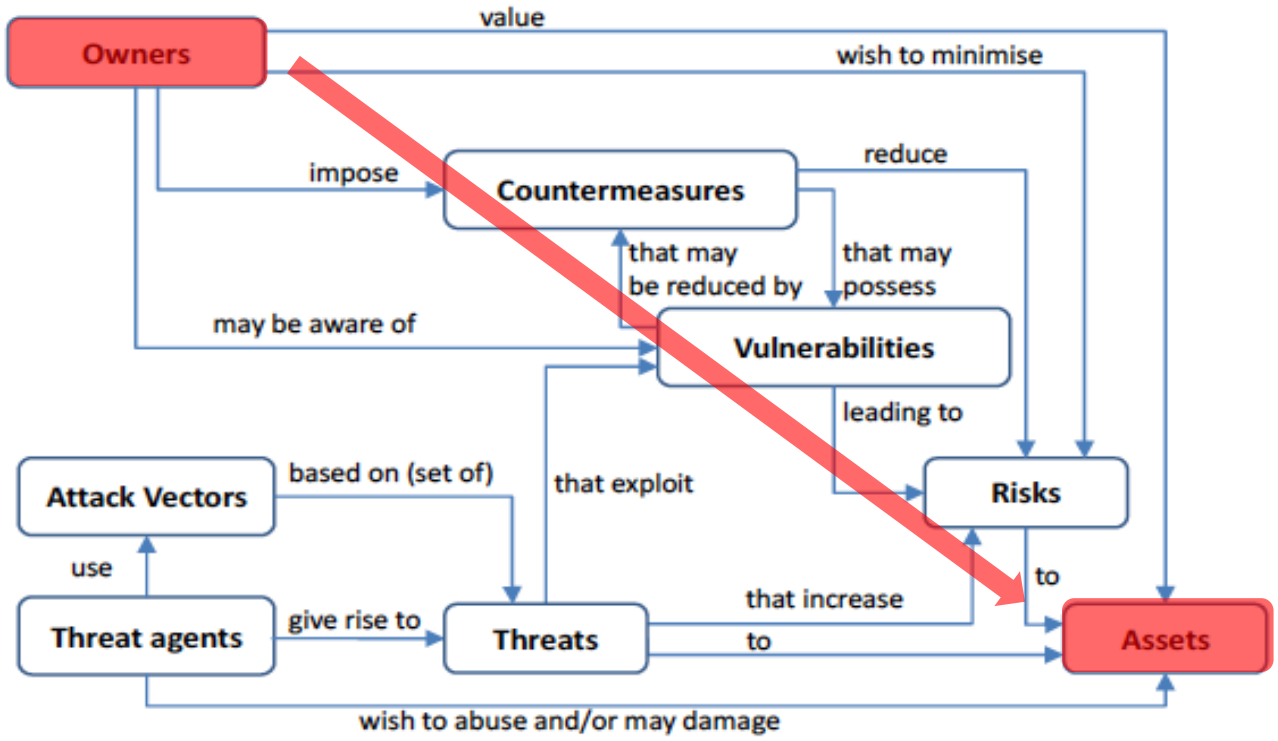


Figure 4: The elements of risk and their relationships according to ISO 15408:2005

Fonte: Enisa Threat Report 2016

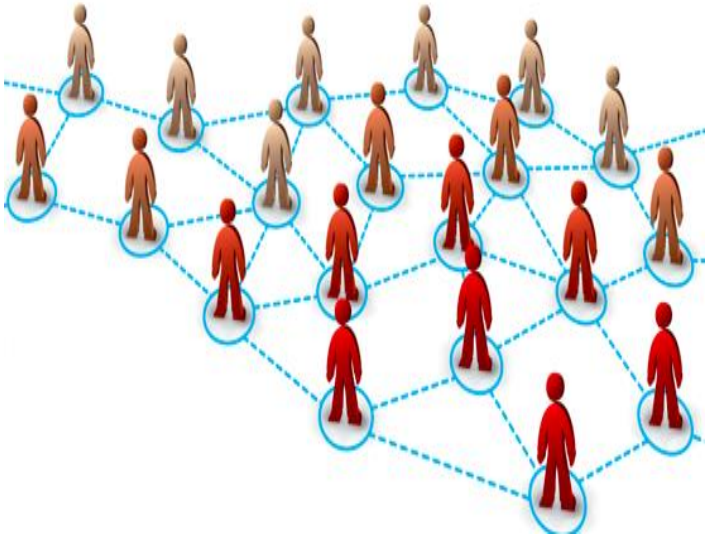
ATTRIBUZIONE DI COMPITI E FUNZIONI ALL'INTERNO DELL'ORGANIZZAZIONE

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 – CHI FA COSA

EDPS: Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments

«…Il vertice dell'organizzazione è responsabile del rispetto delle regole, ma la responsabilità è solitamente assunta a un livello inferiore ("persona responsabile per conto del titolare" / "titolare in pratica ")….»

Operativamente:

***Accountable** è il vertice dell'organizzazione.*

***Responsabile dell'attività** dovrebbe essere del Referente organizzativo - «business owner»*

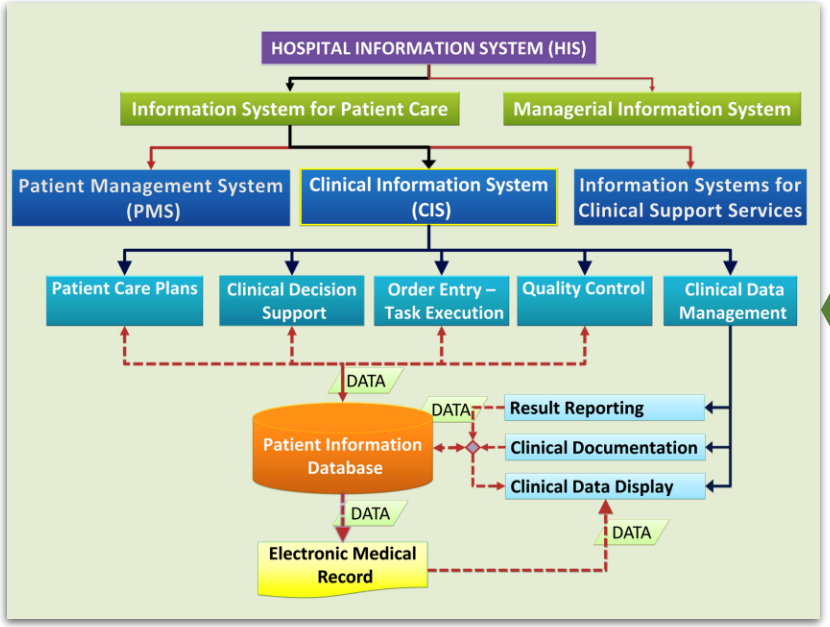
Referente (Owner) soggetto che, nella pratica quotidiana, ha la responsabilità organizzativa del processo che coinvolge le specifiche attività di trattamento.

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

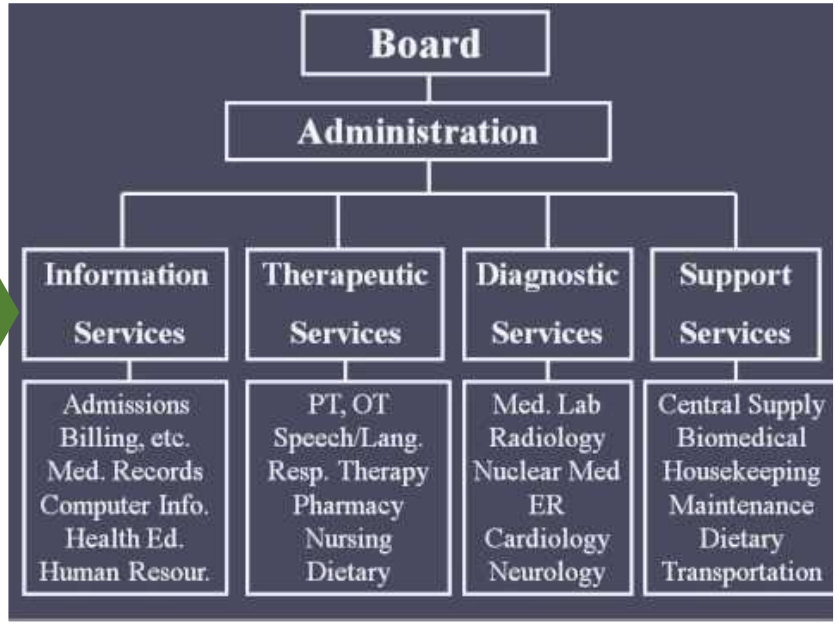
Responsible	Ha l'obbligo di azione e di decisione per il raggiungimento dei risultati richiesti
Accountable	Risponde delle azioni, delle decisioni e della prestazione
Consulted	Contribuisce e fornisce commenti
Informed	Viene tenuto informato delle decisioni prese e del trattamento

Fonte: Elaborazione da: «European Data Protection Supervisor -Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments - RACI matrix DPIA process» - febbraio 2018, p. 4

IDENTIFICARE LE ATTIVITÀ DI TRATTAMENTO IN RELAZIONE AI PROCESSI DELL'ORGANIZZAZIONE



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

RIFERIMENTO ALLE UNITÀ ORGANIZZATIVE REFERENTI (OWNER) DELLE ATTIVITÀ DI TRATTAMENTO

(Article 30 par. 1(a))		(*) *If applicable* **CONTROLLER** CONTACT DETAILS: Name, Address, Email, Telephone **JOINT CONTROLLER** CONTACT DETAILS (*) Name, Address, Email, Telephone **REPRESENTATIVE** CONTACT DETAILS (*) Name, Address, Email, Telephone **DATA PROTECTION OFFICER** CONTACT DETAIL (*) Name, Address, Email, Telephone							
	ORGANIZATION UNIT ("OWNER" OF THE PROCESSING ACTIVITY)	(Article 30 par. 1(b)) PURPOSES OF THE PROCESSING	(Article 30 par. 1(c)) CATEGORIES OF DATA SUBJECTS	(Article 30 par. 1(c)) CATEGORIES OF PERSONAL DATA	(Article 30 par. 1(d)) CATEGORIES OF RECIPIENTS	(*) (Article 30 par 1(e)) TRANSFERS OF PERSONAL DATA TO A THIRD COUNTRY OR AN INTERNATIONAL ORGANISATION	(Article 30 par. 1(f)) TIME LIMITS FOR ERASURE		(Article 30 par. 1(g) TECHNICAL AND ORGANIZATIONAL MEASURES
1									
2									
3									
4									

AGGIORNAMENTO DEL REGISTRO

- E’ opportuno che il registro sia costantemente aggiornato al fine di avere una esatta corrispondenza tra la traccia delle attività di trattamento riportate nel registro e quelle che correntemente avvengono all’interno dell’organizzazione.
- Quando si verifica un cambiamento nel trattamento dei dati personali (a causa di cambiamento organizzativo, tecnico o altra fonte di cambiamento) o viene avviata nuova attività di trattamento, il registro deve essere tempestivamente aggiornato.
- Si raccomanda una revisione periodica delle registrazioni per verificare che tutti gli aggiornamenti necessari siano effettivamente stati eseguiti
- E’ evidente che affinché ciò avvenga in maniera tempestiva:
  - è necessario che sia avviata una preventiva attività di sensibilizzazione interna circa l’importanza dell’aggiornamento del Registro.
  - venga definito un processo organizzativo di notifica interna delle variazioni e conseguente aggiornamento del registro (presumibilmente a cura dei referenti/owner organizzativi delle attività di trattamento)

REGISTRO E RPD

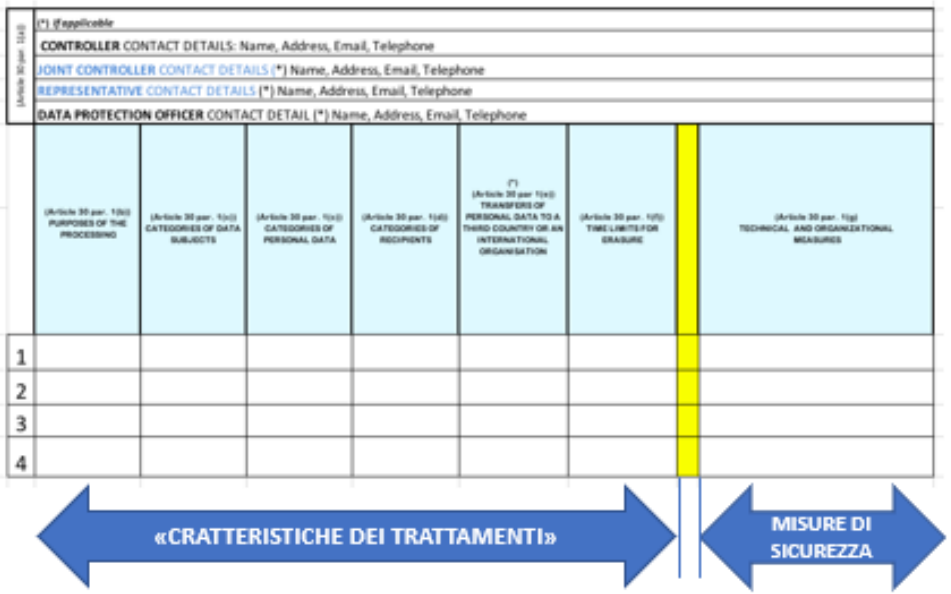
REGISTRO DEI TRATTAMENTI E RPD

Linee-guida sui responsabili della protezione dei dati - WP 243 rev. 01

Il ruolo del RPD nella tenuta del registro delle attività di trattamento

- L'art. 30, primo e secondo paragrafo, prevede che sia il titolare o il responsabile del trattamento, e non il RPD, a "*tenere un registro delle attività di trattamento svolte sotto la propria responsabilità*" ovvero "*un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento*".
- **Nella realtà, sono spesso gli RPD** a realizzare l'inventario dei trattamenti e **tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali.**
- L'art. 39, primo paragrafo, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, **niente vieta al titolare o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività** di trattamento sotto la responsabilità del titolare o del responsabile stesso.
- **Tale registro** va considerato **uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile.**

REGISTRO: L'IMPORTANZA DELL'ANALISI DEI RISCHI



COMPITI DEL RPD Art. 39.2

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 e delle finalità del medesimo.

Sicurezza del trattamento

Articolo 32.1

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

RIFERIMENTI

Manuale RPD – di Douwe Korff & Marie Georges. *Compiti organizzativi* «*Compito 1: La creazione di un registro delle attività di trattamento di dati personali*» - Pag. 170

(Cfr.: https://www.garanteprivacy.it/documents/10160/0/T4DATA+-+Manuale+per+gli+RPD.pdf/bdea3d2d-7bfc-80c5-8f1c-f8c567b44e50?version=1.1)

Manuale RPD

Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea

(Regolamento (UE) 2016/679)

Elaborato per il programma "T4DATA" finanziato dall'UE

(Accordo di sovvenzione n°: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

di

Douwe Korff

Professore Emerito di Diritto Internazionale, Professore associato alla London Metropolitan University, alla Oxford Martin School e all'Università di Oxford

&

Marie Georges

Esperto indipendente sulla protezione internazionale dei dati (Ex-CNIL, Ue, Consiglio d'Europa, ecc.)

Membri del Gruppo FREE - Fundamental Rights Experts Europe

Con il contributo del Garante italiano per la protezione dei dati personali & dei Partner del progetto

(versione approvata dalla Commissione, luglio 2019)

ARC
GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

Cofinanziato dall'Unione Europea

GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Grazie