



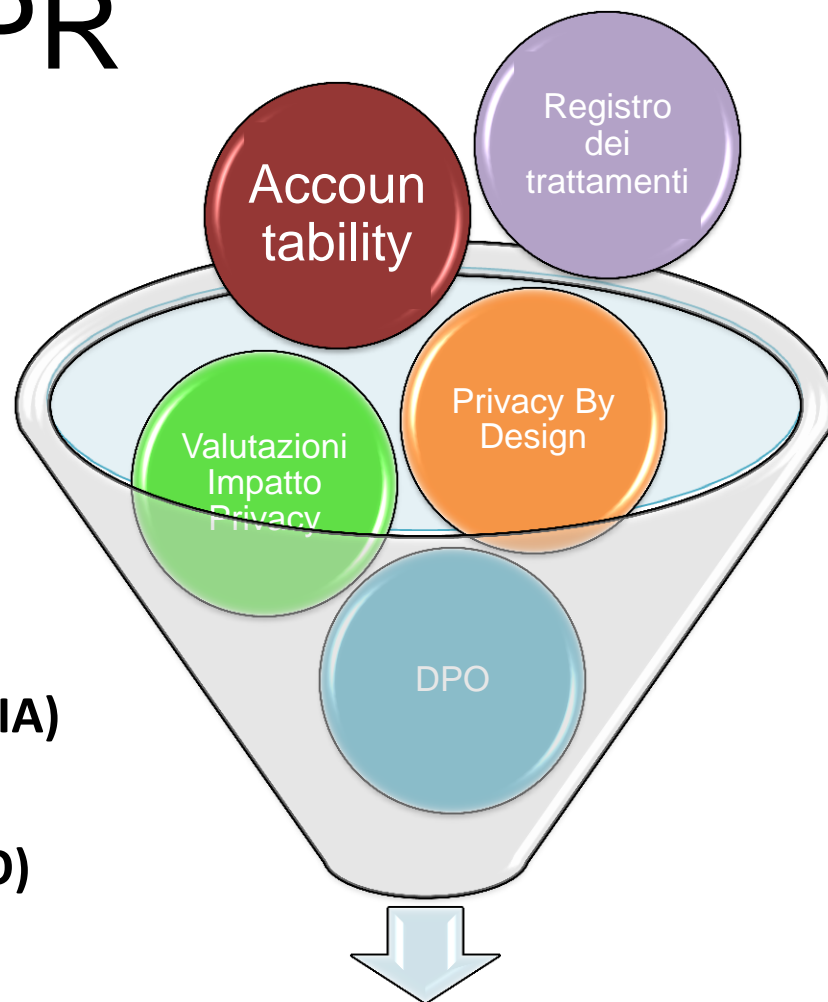
Privacy

L'impatto sul Psn del Regolamento europeo sulla privacy

Monica Attias, Bernardo Palazzi - Istat
Roma 16 novembre 2018

GDPR

- I principali elementi introdotti:
 - Accountability (art. 24)
 - Privacy by design e by default (art. 25)
 - Registro dei trattamenti (art. 30)
 - **Valutazioni impatto Privacy (VIP/PIA) (art. 35)**
 - **Responsabile Protezione Dati (DPO) (art. 39)**
- Elementi necessari per la Conformità al **GDPR**



Conformità GDPR

Responsabile Protezione Dati (DPO) - art. 39

L'RPD deve avere almeno i seguenti compiti:

- **informare e consigliare** riguardo **gli obblighi** sia il titolare che gli incaricati che svolgono trattamento
- **monitorare la conformità** con la **normativa sulla privacy**, in particolare:
 - Modalità per assegnazione delle responsabilità
 - Sensibilizzazione e formazione del personale impegnato in operazioni di trattamento
- cooperare e agire come punto di contatto tra l'autorità Garante e il proprio datore di lavoro
- fornire consulenza ove richiesto per quanto riguarda la valutazione d'impatto sulla protezione dei dati (VIP) e validarne i risultati



GDPR art.35 valutazione impatto

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta nei seguenti casi :

- a) una **valutazione sistematica e globale di aspetti personali** relativi a **persone fisiche**, basata su un **trattamento automatizzato**, compresa la **profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b) il trattamento, su **larga scala**, di **categorie particolari di dati personali** di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

GDPR art.35 valutazione impatto

7. La valutazione contiene almeno:

- a. una **descrizione sistematica** dei **trattamenti previsti** e delle **finalità del trattamento**, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento
- b. una **valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità**
- c. una **valutazione dei rischi per i diritti e le libertà degli interessati**
- d. le **misure previste per affrontare i rischi**, includendo le garanzie, le **misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento**, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

GDPR considerando 84

1. Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.
2. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento.
3. Laddove la **valutazione d'impatto** sulla protezione dei dati **indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare** mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, **prima del trattamento si dovrebbe consultare l'autorità di controllo.**

L'informativa per i trattamenti inclusi nel Psn rilevanza e caratteristiche

- ✓ L'informativa è uno strumento di **trasparenza** riguardo al trattamento dei dati personali e all'esercizio dei diritti

Considerando 39 del GDPR :Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un **linguaggio semplice e chiaro**.

- ✓ Contiene le informazioni necessarie ai sensi dell'art. 13 Dlgs.196/2003 e da maggio del 2018 ai sensi degli artt. 13 e 14 del GDPR

Informativa: cosa cambia con il GDPR

Profili di responsabilità

- ✓ RPD – Responsabile della protezione dei dati
- ✓ I contitolari debbono sottoscrivere un contratto di contitolarità
- ✓ Responsabile «interno» alla propria amministrazione di uno specifico trattamento di dati personali: **soggetto designato dal titolare**
- ✓ Responsabile del trattamento dei dati «esterno»: organo intermedio, ditta, partecipante (contratto)

Profili di responsabilità

Nell'informativa dovranno figurare i dati di contatto del Responsabile della protezione dati RPD. Nel 2018 il **Psn 2018 sarà integrato da una tabella apposita.**

La dichiarazione del soggetto designato dal titolare (prima definito responsabile del trattamento) a svolgere il lavoro nell'ambito del Psn comporta il controllo della veridicità e della correttezza delle informazioni.

Non cambia il ruolo dell'U.S. ai fini del Psn

In caso di lavori affidati ad **ufficio diverso dall'US**, il resp. dell'US attesta di aver verificato la correttezza e le metodologie adottate.

Contitolarità del trattamento (art. 26)

Alcuni Sistemi informativi statistici (SIS) sono svolti in contitolarità

Cosa cambia con il GDPR

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento

L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. **Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.**

Il Responsabile del trattamento dei dati personali

Soggetto che raccoglie le informazioni

- 1 Titolare del lavoro
- 2 Organo intermedio**
- 3 Ditta esterna**

Secondo il REG. UE, le figure in rosso sono responsabili del trattamento per conto del titolare

Soggetti compartecipanti

Ci sono soggetti compartecipanti? Si No

Soggetto compartecipante Regione...../Regioni

Modalità di compartecipazione

Finanziaria

Metodologica-Tecnica

Altro...***trattamento di dati personali***

Tempi di conservazione o criteri per determinarla

Nel Psn si rilevano le caratteristiche dei

dati di input (fonti): i tempi di conservazione sono espressi in mesi

dati di output (microdati statistici): attualmente non si rilevano i tempi di conservazione

I **termini ultimi previsti** per la cancellazione/anonimizzazione delle diverse categorie di dati dovranno essere individuati per tipologia e finalità di trattamento

Ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a **criteri** (es. norme di legge, prassi settoriali) indicativi degli stessi (es. “in caso di contenzioso, i dati saranno cancellati al termine dello stesso”, in caso di rapporto contrattuale, i dati saranno conservati per un periodo fissato