Il Regolamento UE 2016/679 in materia di protezione dei dati personali e valutazioni d'impatto

Politecnico di Torino, 24 novembre 2017

Giuseppe D'Acquisto

Il contesto tecnologico

- Mediazione e neutralità
- Effetti di scala e specializzazione

Tutele giuridiche

- Accountability
  - Incentivi (semplificazioni)
  - Deterrenza (sanzioni)
  - Nuova supervisione (cooperazione)
  - Nuovi obblighi
  - Controllo distribuito (nuovi diritti)

Le valutazioni d'impatto

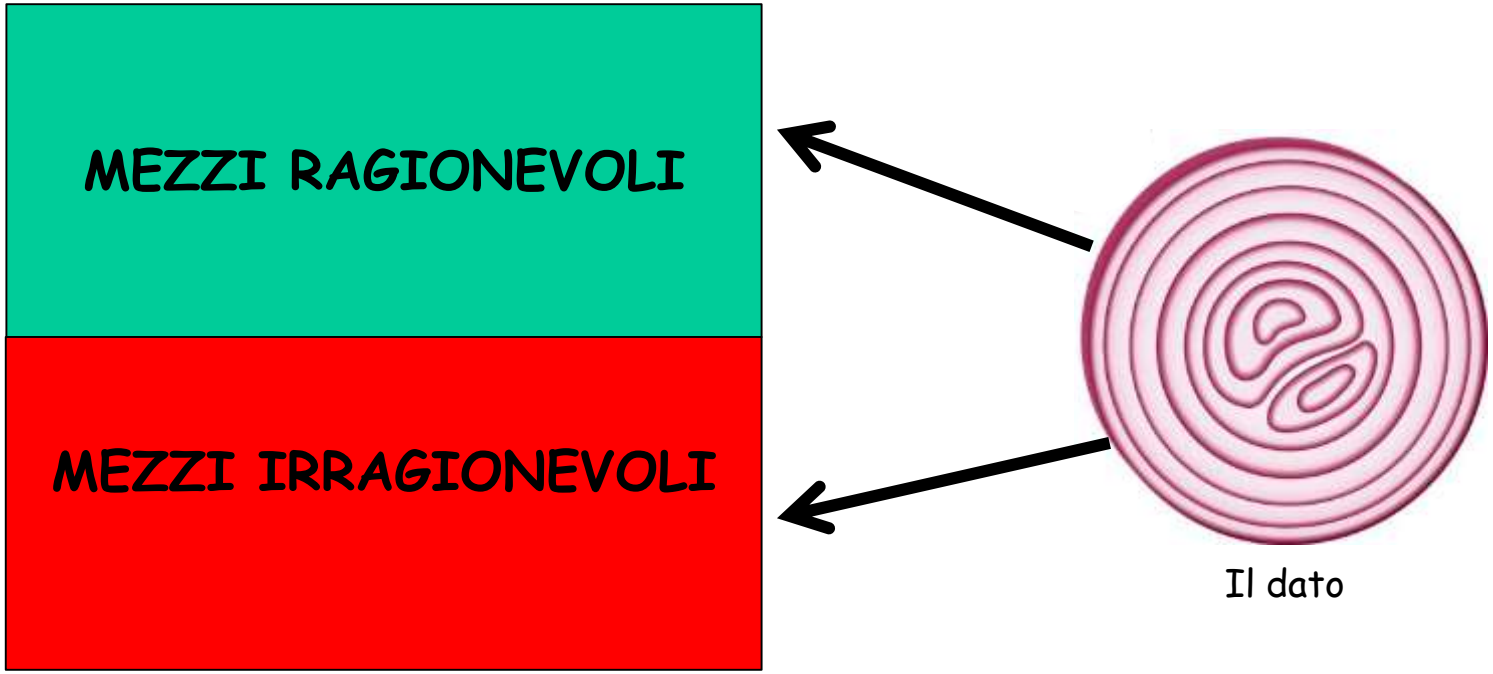
- Strumenti di accountability
  - Art. 25 Privacy by Design (zero impact)
  - Art. 32 Sicurezza (ex ante impact)
  - Art. 33-34 Data Breach (rimediare all'impatto)
  - Art. 35-36 DPIA (ex ante high risk + consultation)

Art. 25 Privacy by Design

- È possibile effettuare trattamenti su dati "minimizzati" fino al punto da non consentire l'identificazione diretta o indiretta di una persona?

  - Considerando (26): …Per stabilire l'identificabilità di una persona è opportuno **considerare tutti i mezzi**, come l'individuazione, **di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi** per identificare detta persona fisica direttamente o indirettamente…

Mezzi ragionevoli e irragionevoli



Cosa è ragionevole?

- Ogni valutazione sulla ragionevolezza del mezzo dovrà tener conto di elementi soggettivi, che possono variare in ragione del contesto
- Elementi di cui tenere conto:
  - Motivazione dell'attaccante
  - Status degli interessati
  - Capacità tecniche dell'attaccante
  - Disponibilità di
    - Risorse economiche
    - Tempo
    - Informazione ausiliarie
  - Variabilità nel tempo (è un processo)

Test di compatibilità

- Per evitare impatti indesiderati sull'interessato:
  1. No Single out
  2. No linkability
  3. No inference

Come evitare impatti sulla persona

- La distorsione è una famiglia di tecniche che modifica la veridicità dei dati al fine di eliminare, ove possibile, il legame che esiste tra il dato puntuale e la persona, ad esempio mediante l'aggiunta di "rumore" statistico ai loro valori
- La generalizzazione consiste nel diluire gli attributi, ossia gli elementi costitutivi dei dati delle persone interessate, modificandone la scala o ordine di grandezza (vale a dire, una regione anziché una città, un mese anziché una settimana, ad esempio). L'incertezza in questo caso è legata al fatto che quanto più lasca è la scala dei valori degli attributi, tanto maggiore è il numero di interessati potenzialmente riferibili a un certo attributo "generalizzato", in modo da rendere via via meno probabile l'attribuzione del dato alla persona.

Art. 32 Sicurezza

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- Dall'approccio esaustivo all'approccio «risk based»

		IMPACT LEVEL		
		Low	Medium	High / Very High
Threat Occurrence Probability	Low			
	Medium			
	High			

La sicurezza come principio (art. 5)

- Quale impatto sulla persona

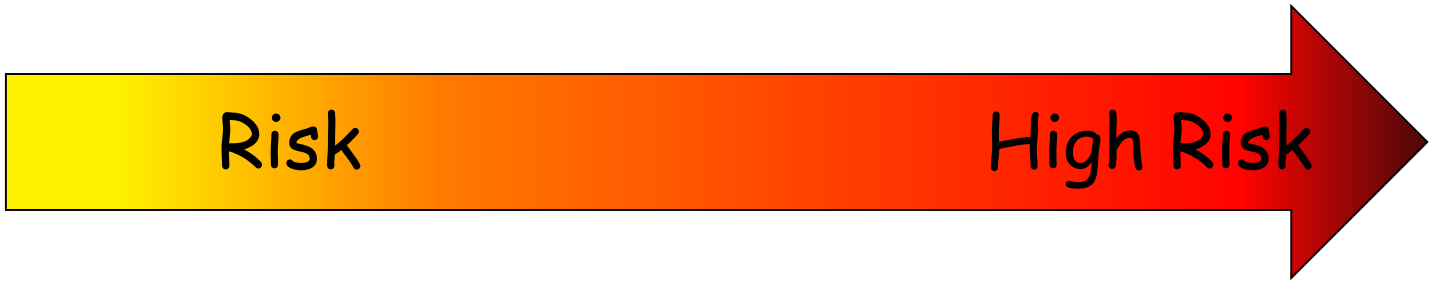
LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Guidelines for SMEs on the security of personal data processing
ENISA Report 2016

Art. 33-34 Data Breach

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- Art 4(12) «violazione dei dati personali»:la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;



Rimediare all'impatto

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- Il titolare del trattamento notifica la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche
- Cosa notificare all'Autorità
  - la natura della violazione (categorie e numero di interessati in questione
  - il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni
  - le probabili conseguenze della violazione dei dati personali
  - le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Rimediare all'impatto

- Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo
- Esenzioni
  - il titolare del trattamento ha messo in atto misure tecniche e organizzative destinate a rendere i dati personali non intellegibili
  - il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati
  - detta comunicazione richiederebbe sforzi sproporzionati
- Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere che vi provveda

Art. 35-36 DPIA

- Quando il rischio è elevato?
- Esempi (art. 35(3)):
  - una valutazione sistematica e globale di aspetti personali (profilazione)
  - il trattamento, su larga scala, di categorie particolari di dati personali (dati sensibili)
  - la sorveglianza sistematica su larga scala di una zona accessibile al pubblico
- Eccezioni:
  - se le finalità del trattamento sono molto simili a quelli del trattamento per cui è già stata condotta una DPIA
  - se il trattamento è stato sottoposto a verifica da parte di un'autorità di controllo prima del maggio 2018
  - se un trattamento trova la propria base legale nel diritto dell'Ue o di uno Stato membro, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta (art. 35, paragrafo 10)
  - se il trattamento è compreso nell'elenco facoltativo (redatto dall'autorità di controllo ai sensi dell'art. 35, paragrafo 5) dei trattamenti per i quali non è necessario procedere alla DPIA.

Criteri

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

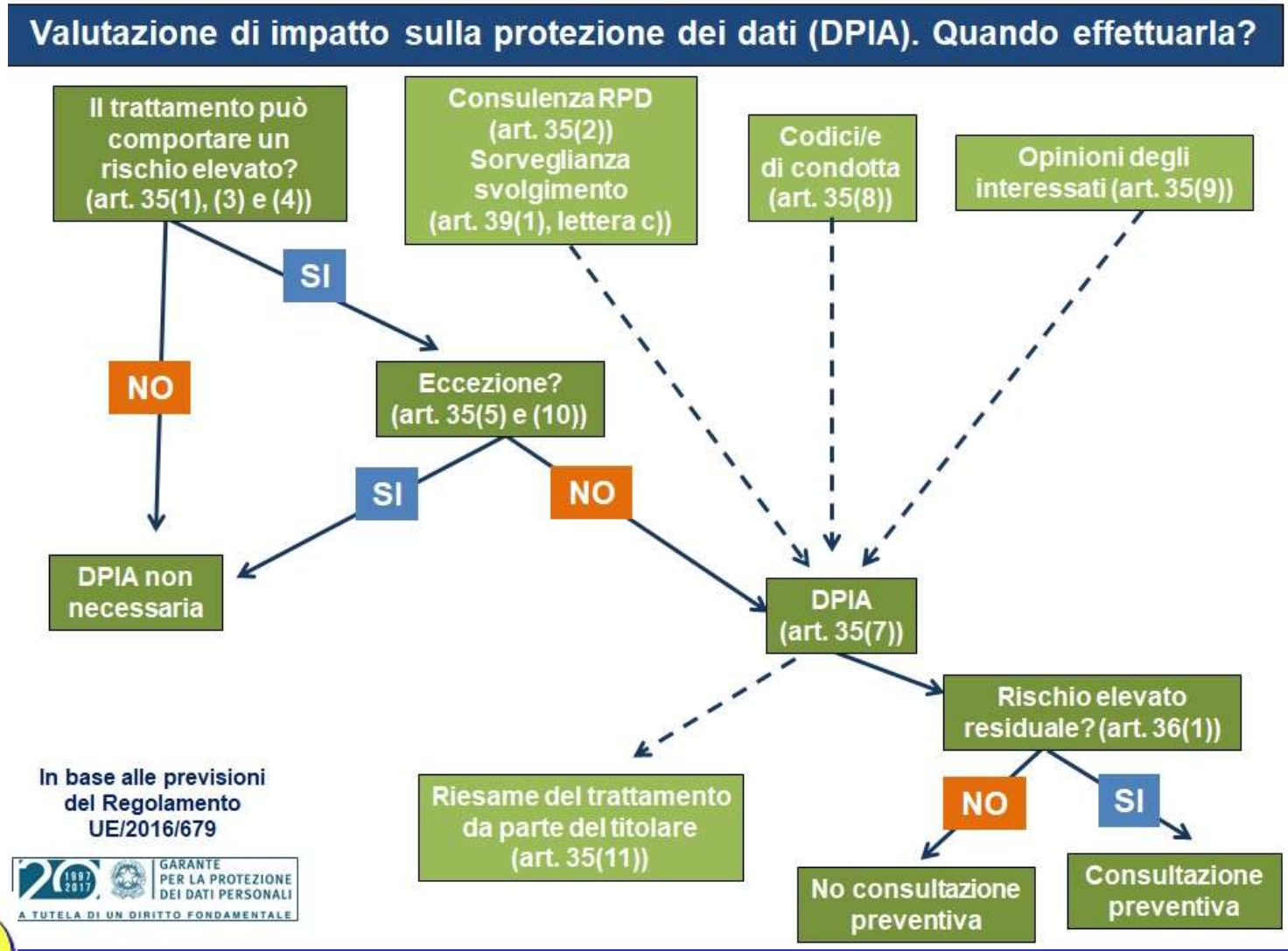
1. Trattamenti valutativi o di scoring
2. Decisioni automatizzate che producono significativi effetti
3. Monitoraggio sistematico
4. Dati sensibili o dati di natura estremamente personale
5. Trattamenti di dati su larga scala
   - a. numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;
   - b. volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;
   - c. durata, o persistenza, dell'attività di trattamento;
   - d. ambito geografico dell'attività di trattamento
6. Combinazione o raffronto di insiemi di dati
7. Dati relativi a interessati vulnerabili
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative

mmetrie e difficolta nell'esercizio dei diritti

Gli elementi di una DPIA

Il processo di valutazione d'impatto

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



I limiti della valutazione d'impatto

- Alla valutazione d'impatto possiamo chiedere soltanto che non si ripetano in futuro impatti già osservati in passato
- Non possiamo chiedere che non si presentino in futuro impatti non noti
- La DPIA è un processo permanente, soprattutto se si ha a che fare con un trattamento dinamico e soggetto a continue trasformazioni. Lo svolgimento della DPIA è dunque un processo continuativo e non un'attività una tantum.

Grazie

g.dacquisto@gpdp.it