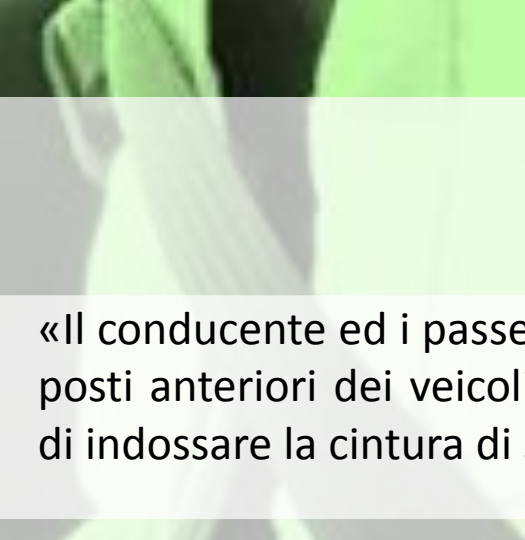


# Data Protection by default & by design l'accountability di titolari e responsabili del trattamento dei dati personali

XIV INCONTRO COMPLIANCE

Il Regolamento europeo UE 2016/679 in materia di protezione dei dati personali: le  
principali novità per imprese e soggetti pubblici

Emanuele Greco  
 Opentech



# 1988

«Il conducente ed i passeggeri occupanti i posti anteriori dei veicoli hanno l'obbligo di indossare la cintura di sicurezza»



# 2003

«È vietato fumare nei locali chiusi, ad eccezione di quelli privati non aperti ad utenti o al pubblico e quelli riservati ai fumatori e come tali contrassegnati»



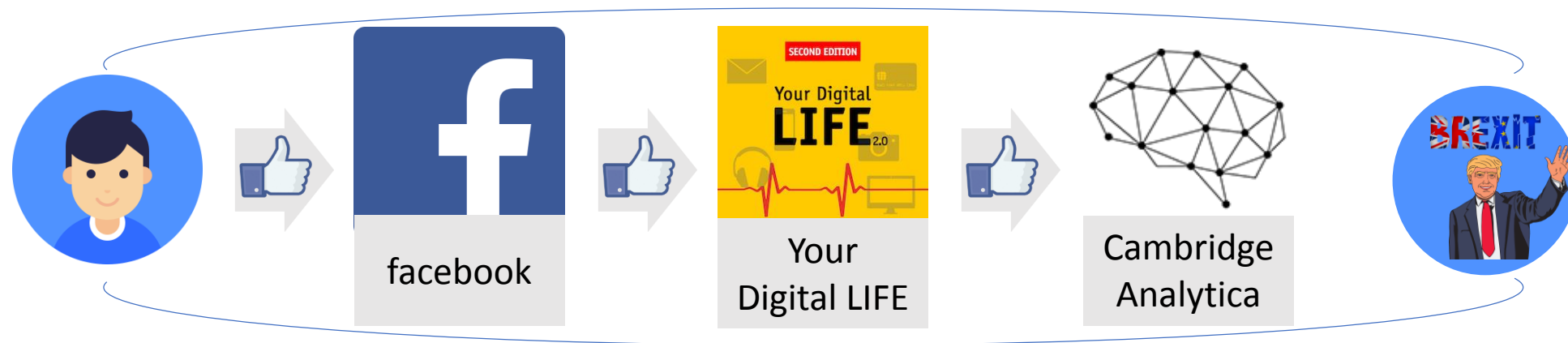
# 2009

«E' fatto obbligo a chiunque conduca il cane in ambito urbano raccoglierne le feci e avere con se' strumenti idonei alla raccolta delle stesse»



**una nuova norma...**

# il caso Cambridge Analytica



*Avendo a disposizione solamente "Mi piace" messi su Facebook per conoscere la personalità di un soggetto*  
**70 like** sono sufficienti per sapere più cose rispetto ai suoi **amici**,  
**150 like** per saperne di più dei **genitori** del soggetto,  
**300 like** per superare le conoscenze del suo **partner**.

*Michal Kosinski, ideatore dell'algoritmo*



Strumenti tecnologici consentono di ottenere **risultati non immaginabili** nel momento in cui sono forniti e raccolti i dati.

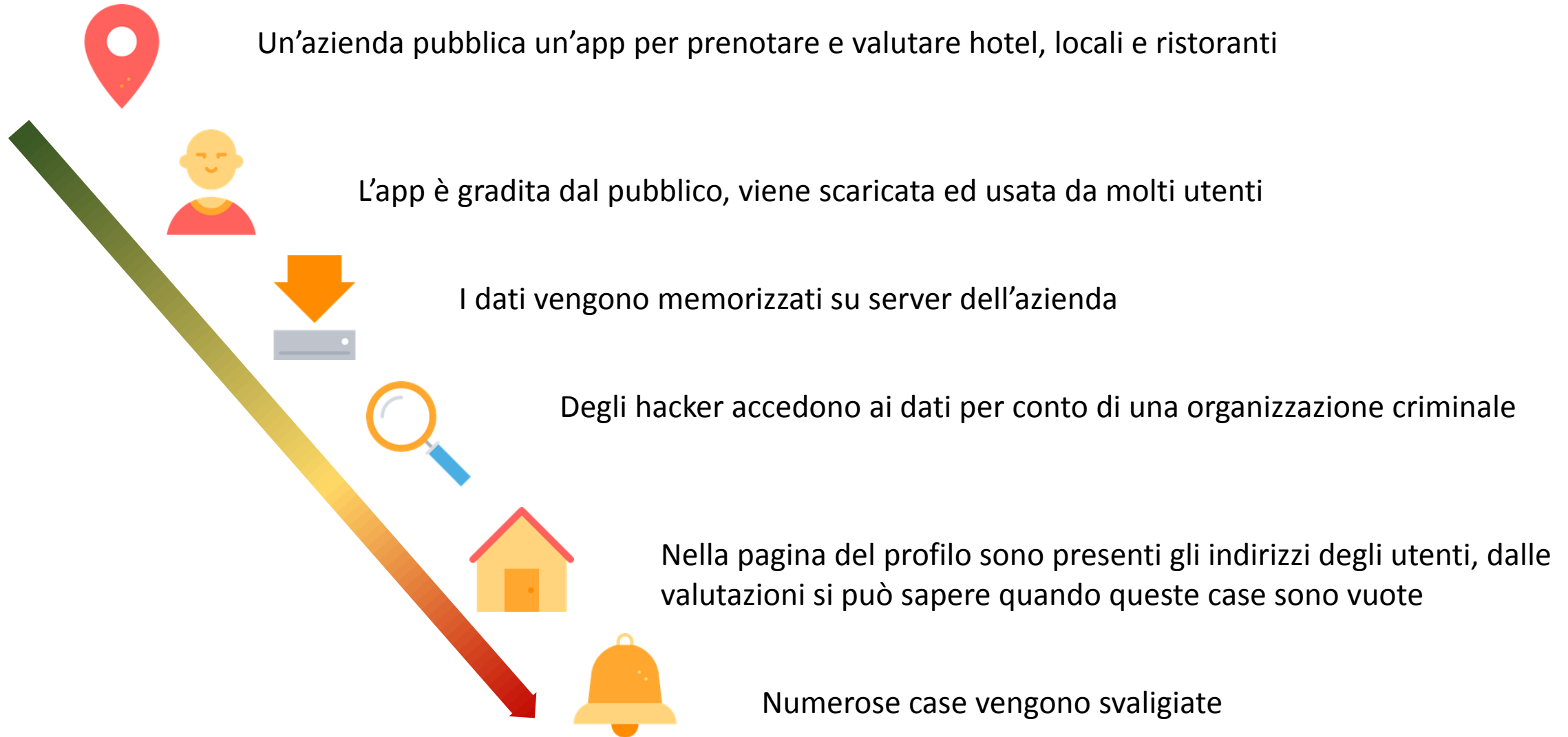
# il caso Cambridge Analytica

2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021



Il GDPR garantisce che vicende come questa non possano più accadere, ma obbliga il Titolare alla massima trasparenza nei confronti degli interessati.

# un «furto» di informazioni



# un «furto» di informazioni

Chi è il responsabile di questo servizio?

Si era compresa la criticità di queste informazioni?

Accountability  
Registri dei trattamenti

DPIA – Data Protection Impact Assessment

**GDPR - Privacy by design**  
evitare che l'incidente succeda e ridurre le conseguenze

Quali sono state le precauzioni adottate?

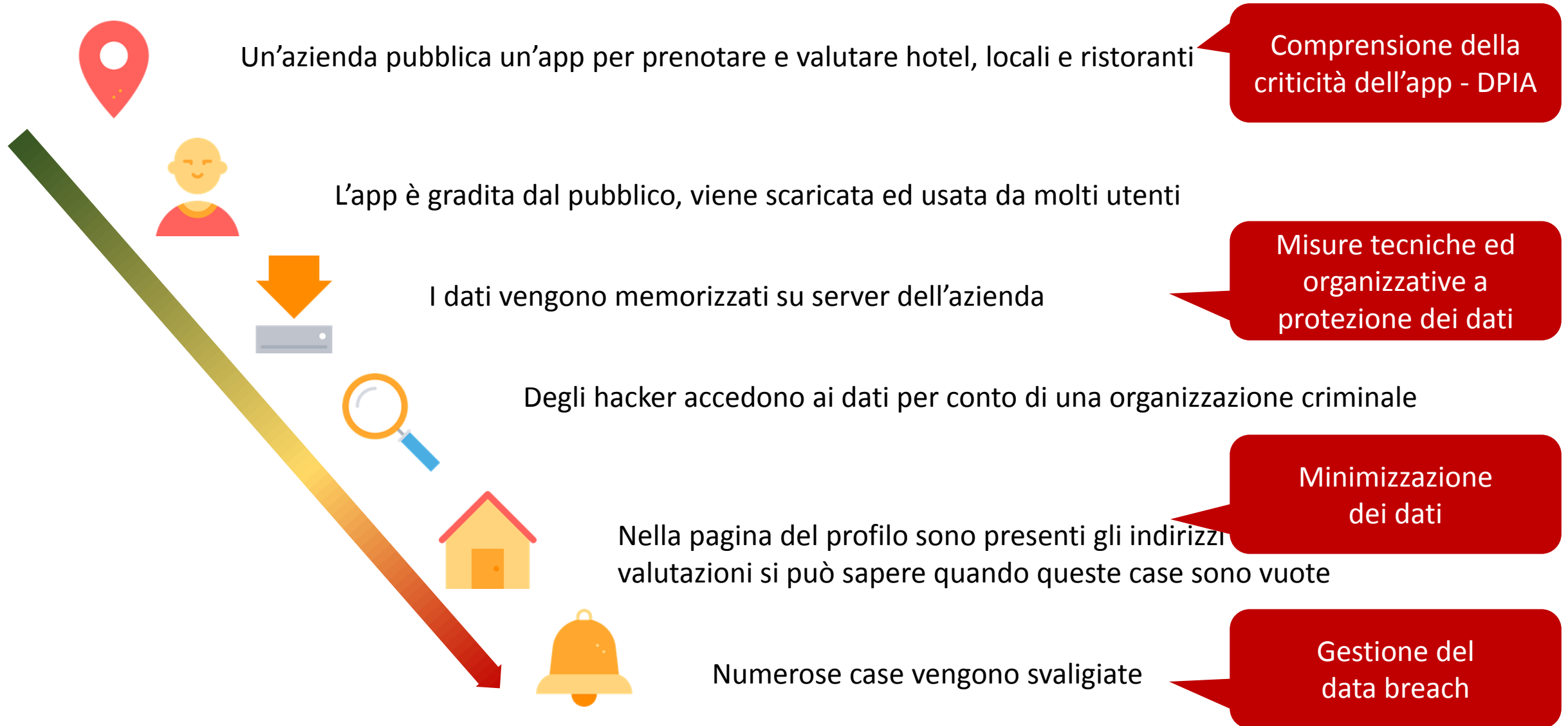
Cosa fare adesso?

Misure tecniche ed organizzative  
Privacy by default

Data breach management

Numerose case vengono svaligate

# un «furto» di informazioni



# Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

## 1. Privacy by design

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.



# Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

## 2. Privacy by default

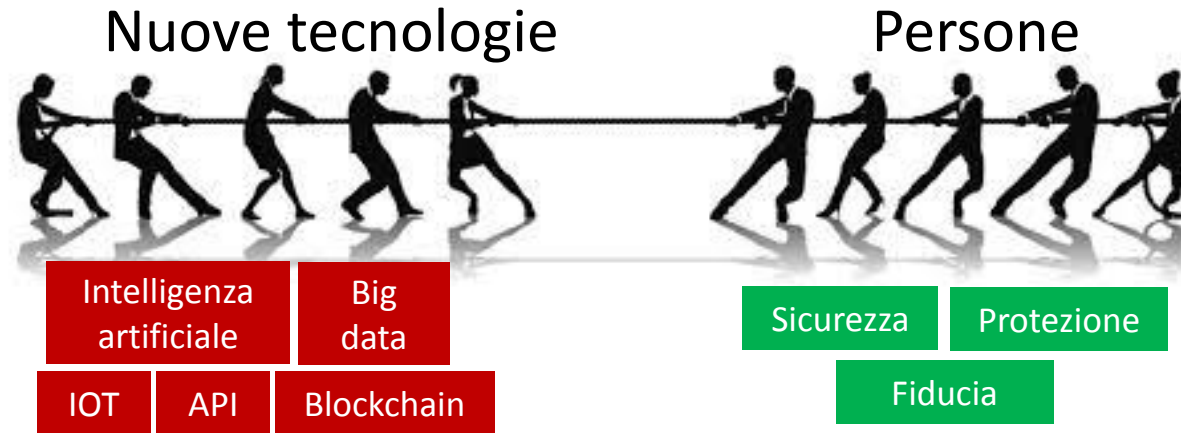
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

# Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

## 3. Conformità ai requisiti della Privacy by design e by default

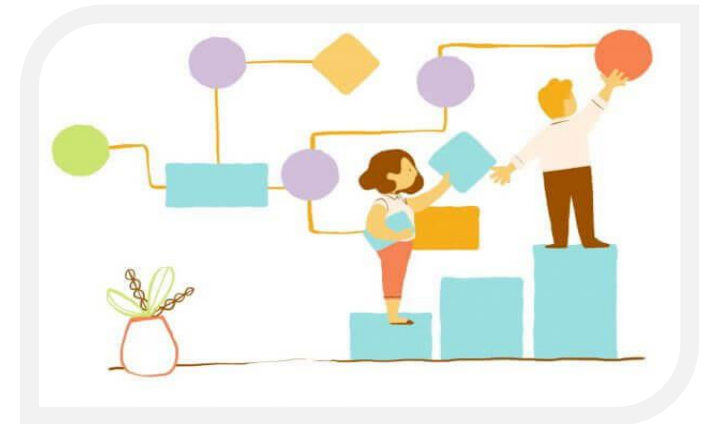
Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

# la privacy by design



Sanzione - attività per  
**prevenire la sanzione**

Progettualità per  
comprendere e  
**prevenire i problemi**



# un sistema di gestione per la privacy

<b>Esigenza</b>	Adeguamento al GDPR [evitare le sanzioni!]
<b>Strategia</b>	Privacy by design: gestione «progettuale»
<ul style="list-style-type: none"><li>- Trattamento di dati personali</li><li>- Informative e consensi</li><li>- Organizzazione e sicurezza informatica</li><li>- Gestione delle terze parti</li><li>- Diritti e richieste dell'interessato</li><li>- Violazioni di dati personali</li></ul>	<b>Consapevolezza</b>
	<b>Organizzazione</b>
	<b>Formazione</b>
	<b>Strumenti</b>
<b>Risultato</b>	L'azienda «funziona» meglio Fiducia da parte di utenti e clienti ...Sanzioni evitate

# Data Protection by default & by design l'accountability di titolari e responsabili del trattamento dei dati personali

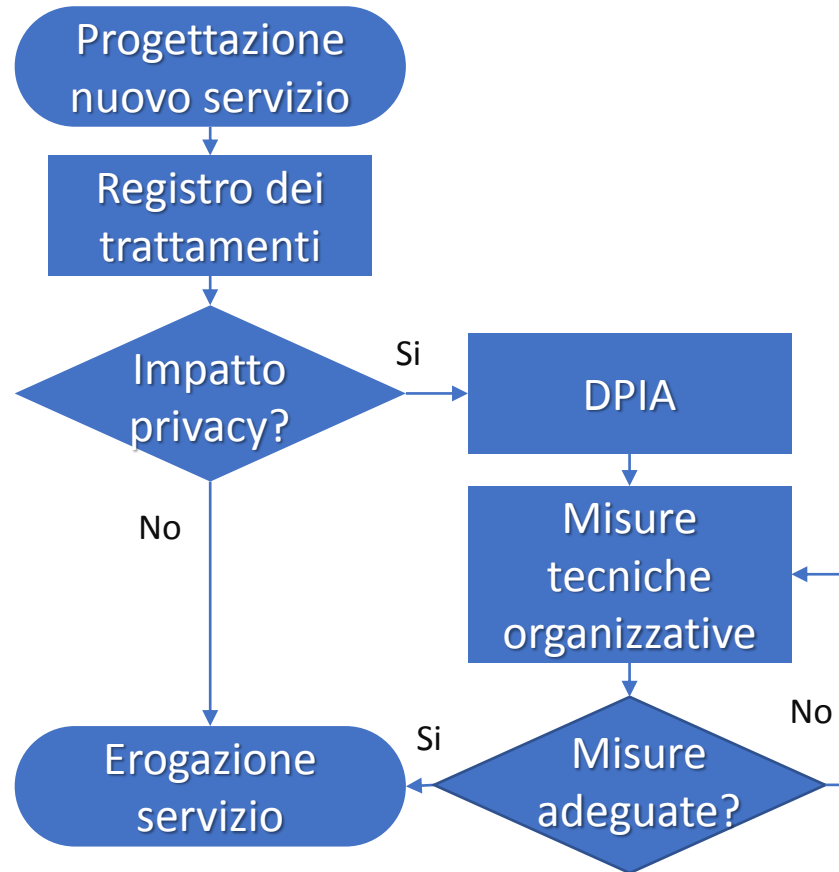
XIV INCONTRO COMPLIANCE

Il Regolamento europeo UE 2016/679 in materia di protezione dei dati personali: le  
principali novità per imprese e soggetti pubblici

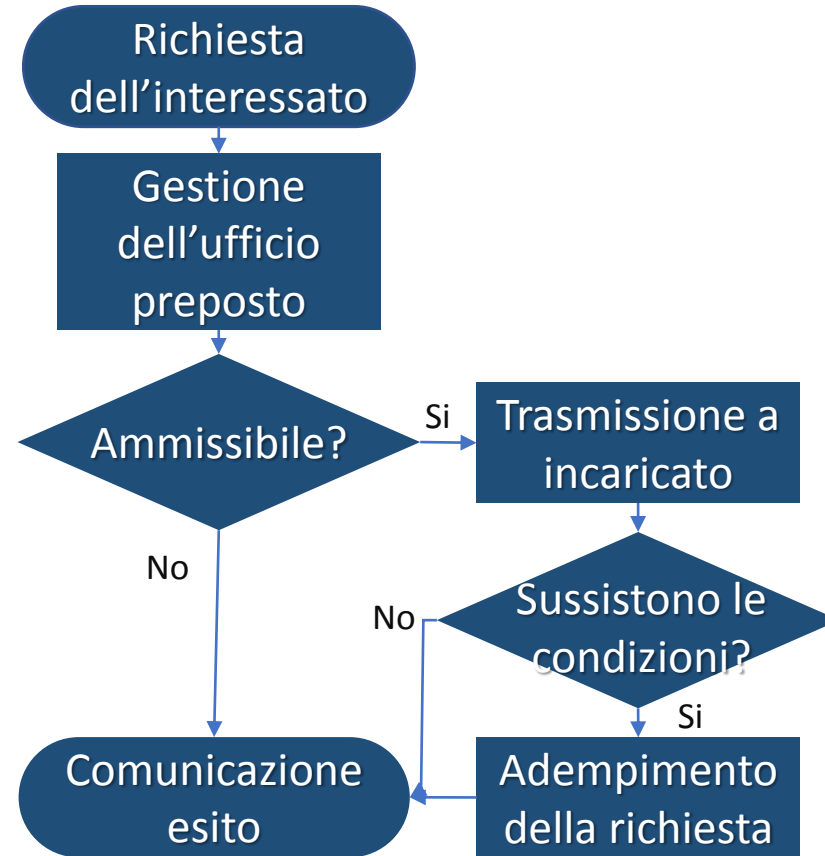
Emanuele Greco  
 Opentech

# un sistema di gestione per la privacy

## Trattamento di dati personali



## Diritti e richieste dell'interessato



# un sistema di gestione per la privacy

## Violazione di dati personali



## Documentazione cartacea

