



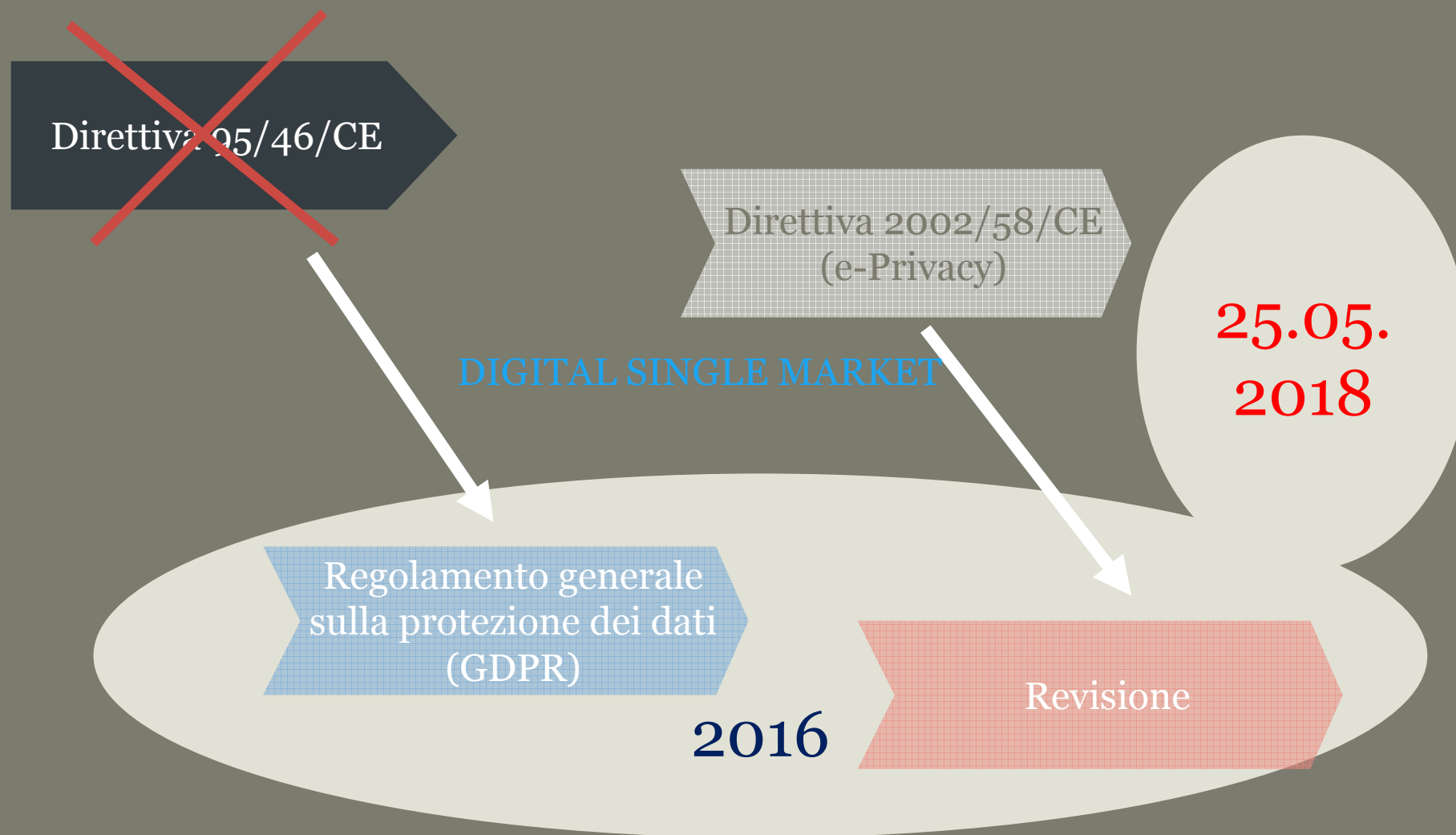
Il Regolamento (UE) 2016/679 e la  
digitalizzazione della PA: quale  
impatto? **& Bird & Bird**

*Roma – 5 ottobre 2016*

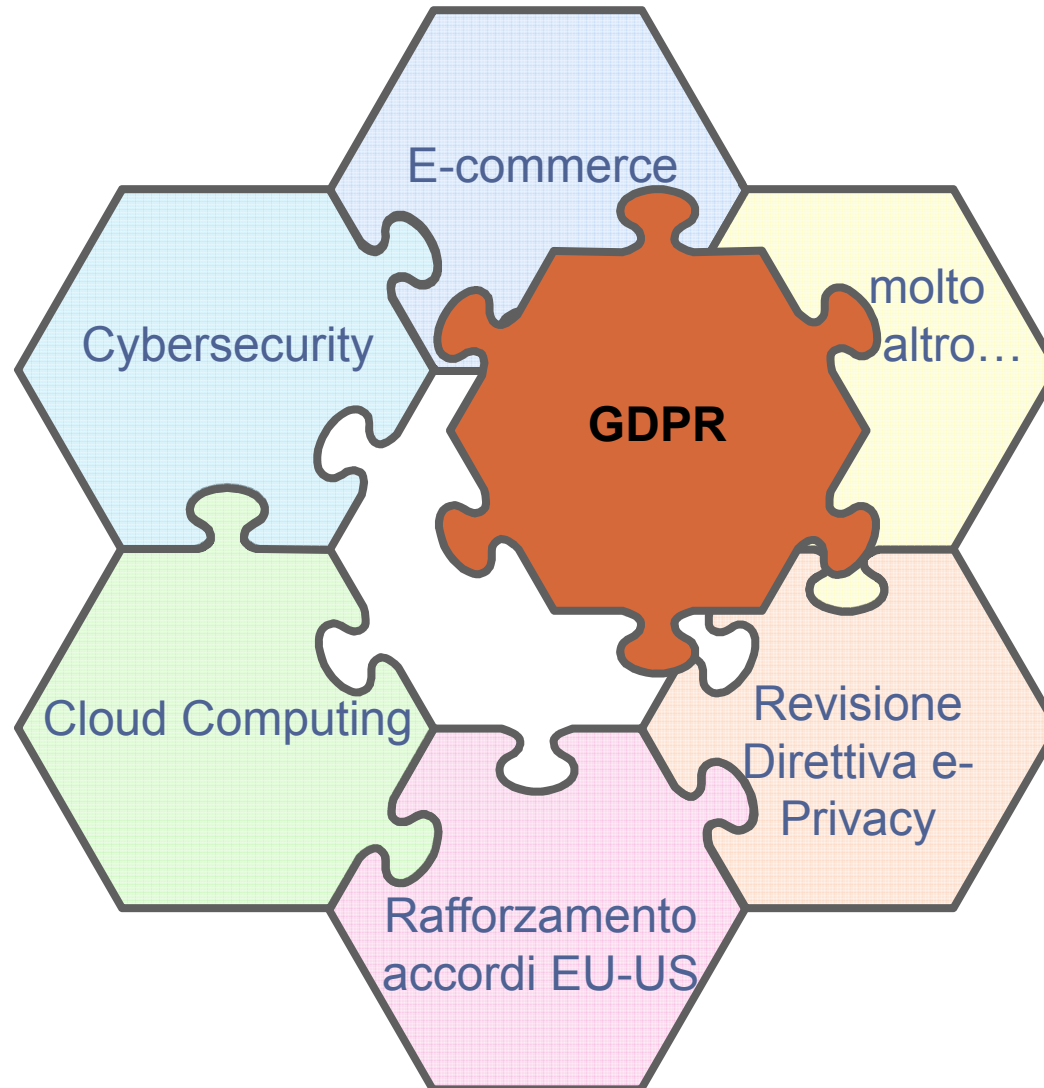
*Avv. Debora Stella*

*Studio Legale Bird & Bird*

# EU: Dalle origini ad oggi



# Tutto al proprio posto...



## Dato e sicurezza: esplorare e capitalizzare

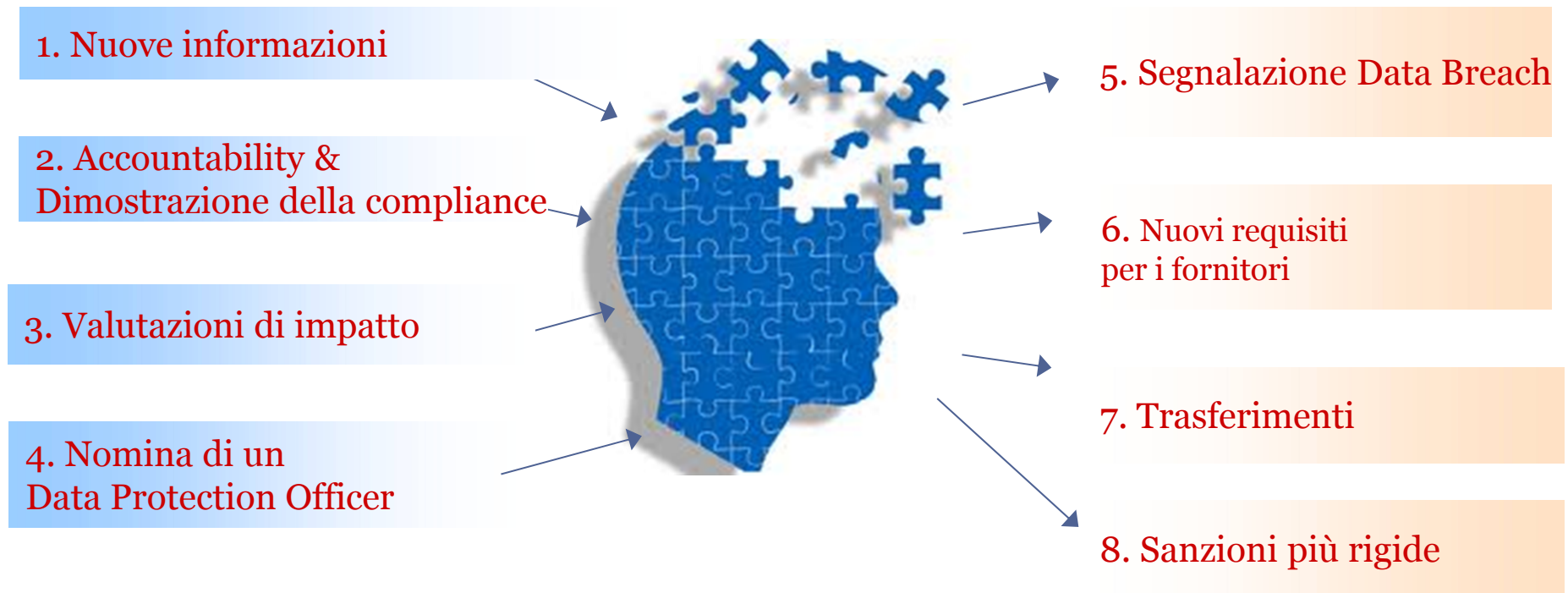
Acquisire il controllo reale ed effettivo sui dati personali = crescita e maggiori opportunità ma anche maggiore fiducia da parte dei cittadini



# Familiarizzare con il Regolamento...

- 1 Regolamento vs 28 leggi nazionali → Maggior **uniformità** applicativa (ma è vero?) + maggior certezza + applicazione diretta
- “One Stop Shop” se la materia non ha rilevanza puramente nazionale, l’autorità di controllo capofila avrà un ruolo centrale
- Ambito di applicazione **territoriale più esteso**
- **Obblighi diretti** per i **responsabili** del trattamento
- **Nuovi concetti**: es. Pseudonimizzazione
- Più trasparenza e più responsabilizzazione (interna e tra soggetti che collaborano nel trattamento)

# I principali 8 impatti del Regolamento



•Prepararsi al Cambiamento

# 1. Nuove informazioni per gli interessati



- **Obbligo di informare gli interessati anche in merito a:**
  - ✓ Tempi di conservazione dei dati
  - ✓ Origine dei dati
  - ✓ Diritto alla portabilità dei dati e restrizioni
  - ✓ Diritto ad adire l'autorità di controllo competente
  - ✓ Legittimo interesse perseguito (legittimo interesse che non si applica però alle pubbliche amministrazioni)
- **Nuovi (?) diritti**
  - ✓ Diritto all'oblio
  - ✓ Diritto alla limitazione del trattamento
  - ✓ Diritto alla portabilità dei dati (a certe condizioni)
  - ✓ Diritto di opporsi a processi di trattamento automatizzati

## 2. Accountability al posto delle notifiche

### To Do List

Documentare (> 250 dip. o attività rischiose)	Privacy by design e by default	Valutazioni di Impatto	Audit
Conservare documentazione e relativa alle operazioni di trattamento (sostituisce obblighi di notifica)  + certificazioni volontarie	Policy & procedure per garantire compliance, specialmente a fini di minimizzazione e dei dati  Privacy by design  (solo per i titolari)	Solo per “attività rischiose”	Audit indipendente per verificare le procedure

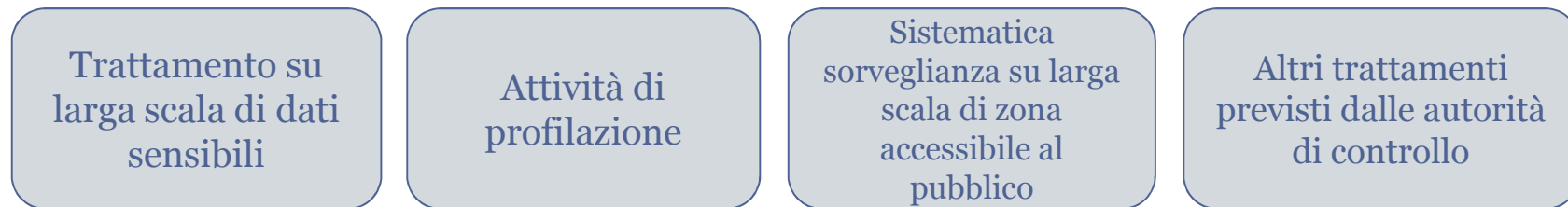
- Assegnare responsabilità e budget per programmi di compliance
- Implementare programmi di compliance
- Monitorare, e conformarsi a, linee guida e codici delle autorità di controllo
- Preparare registro delle attività

A carico di titolari e responsabili



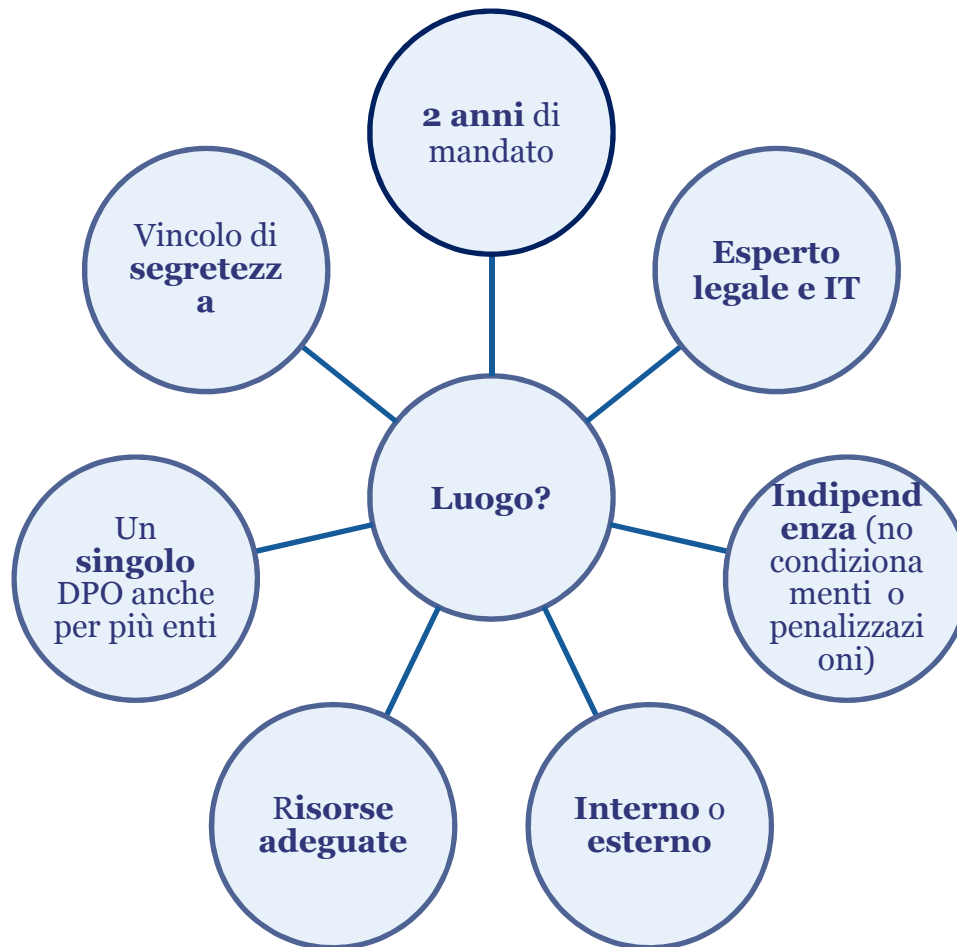
### 3. Valutazioni d'impatto

- Attività di audit effettuata su aree specifiche per identificare e minimizzare i rischi di non conformità
- **Obbligo** in caso di trattamenti che possano comportare **rischi elevati** per la libertà e dignità dei cittadini, es.:



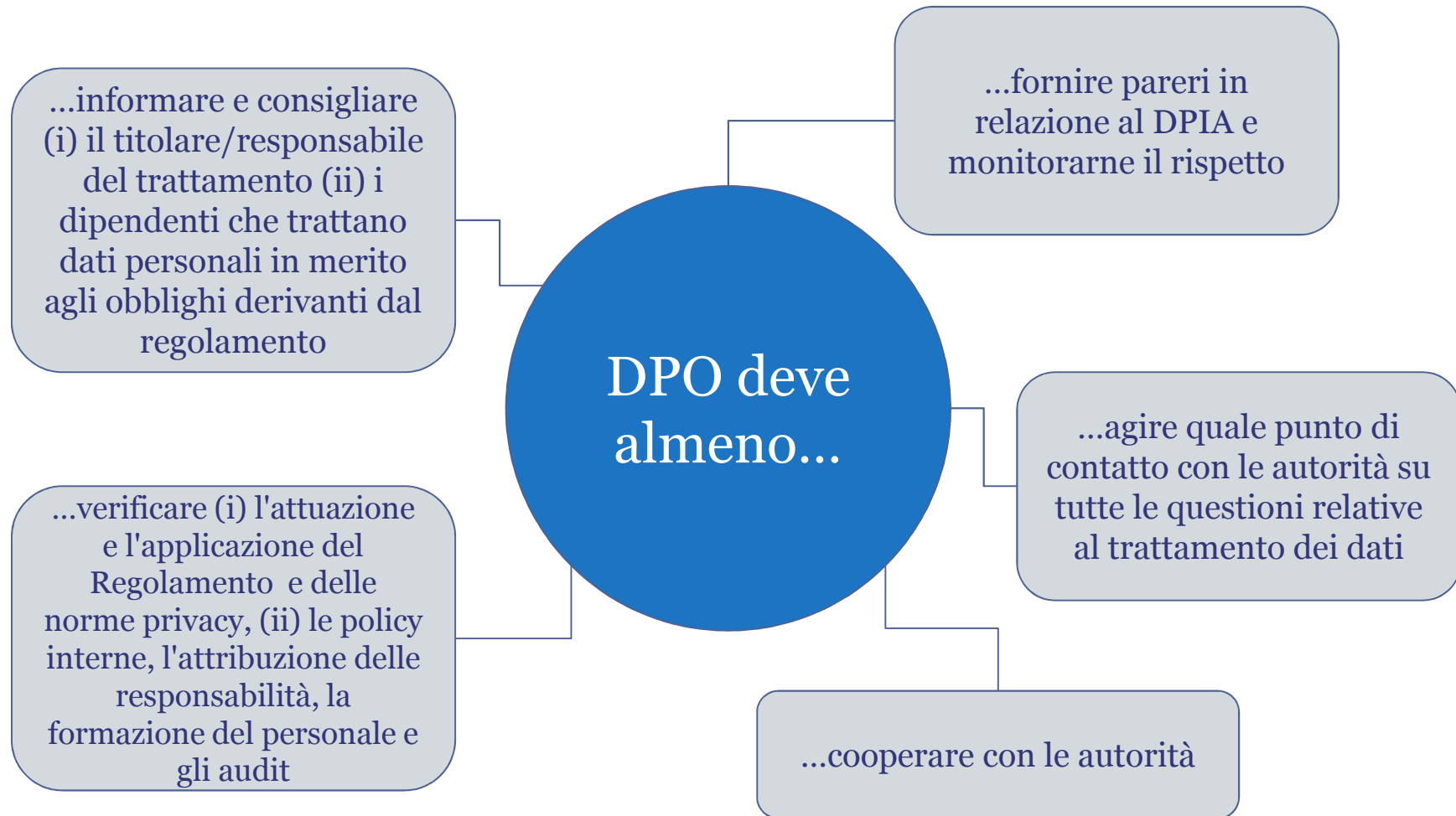
- Contiene almeno:
  - Una descrizione specifica dei trattamenti e delle finalità
  - Una valutazione di proporzionalità del trattamento, dei rischi connessi e delle misure di mitigazione dei rischi (specie misure di sicurezza, garanzie)
- Identificazione delle aree di rischio elevato: definita dalle autorità di controllo
- Raccomandato estenderne l'implementazione oltre i casi strettamente obbligatori

## 4.1. Quando occorre nominare un DPO: attività di trattamento particolarmente rischiose?

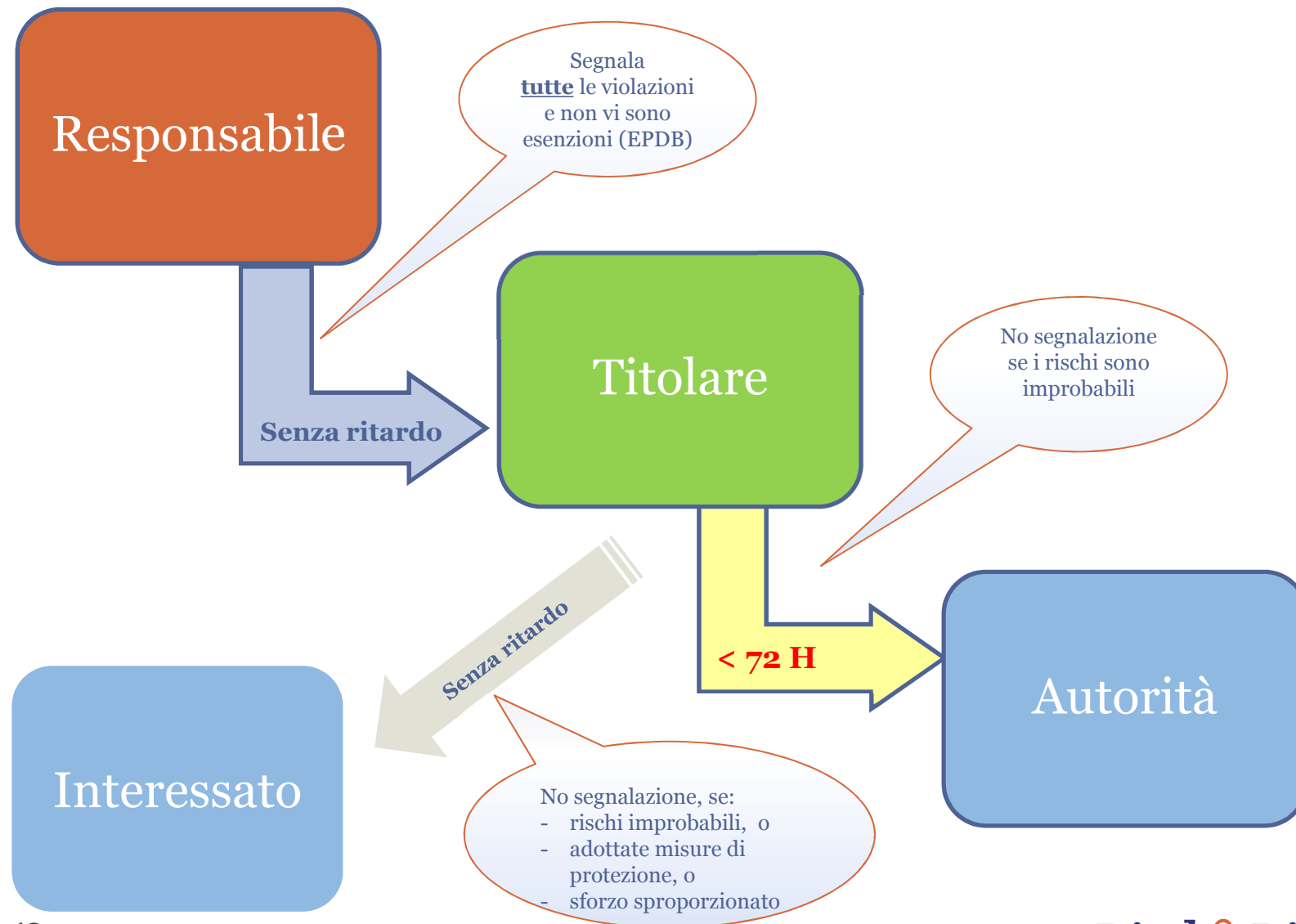


- Monitoraggio sistematico e regolare "degli individui" su larga scala
- Trattamenti di dati sensibili o giudiziari su "larga scala"
- Trattamenti effettuati da una **pubblica amministrazione**

## 4.2. Principali compiti del DPO



## 5.1 Segnalazioni di Data Breach



## 5.2 Notifiche data breach: quali differenze tra N&IS e GDPR


### To Do List

- Obiettivi differenti:
    - N&IS: proteggere i servizi critici rispetto a importanti compromissioni del servizio stesso
    - GDPR: proteggere i dati personali rispetto alla perdita, modifica, comunicazione ecc.
  - Tempistiche strettissime:
    - N&IS: senza ritardo proteggere i servizi critici rispetto a importanti compromissioni del servizio stesso
    - GDPR: entro 72 ore dalla conoscenza (comunicazione del titolare all'autorità)
- ☑ Definire o aggiornare procedure per rilevare e gestire incidenti di sicurezza sui dati
  - ☑ Valutare misure di pseudonimizzazione e crittografia, se già non necessarie
  - ☑ Verificare e integrare, se necessario, i contratti con i fornitori con previsioni contrattuali per la gestione degli incidenti di sicurezza e definire gli obblighi di cooperazione


## 6.1 Nuovi requisiti per i fornitori

- **Obblighi diretti tra cui:**

- ✓ Obblighi di **documentazione**: policy sul trattamento dei dati, policy di sicurezza, procedure atte a dimostrare la compliance con il Regolamento...
- ✓ Tenuta di un **registro delle attività di trattamento** per ciascun cliente-titolare (Art.30.2)
- ✓ Innalzamento requisiti di **sicurezza sui dati** adottando misure specifiche parametrare ai rischi, tra cui, pseudonimizzazione, crittografia, ...(Art.32)
- ✓ Obbligo di segnalazione al titolare dei **Data breach** (Art 33.2)



Direttamente soggetti a poteri di investigazione, di controllo e sanzionatori da parte delle autorità di controllo (Art.58)

- 
- **Responsabilità diretta** verso gli interessati per i danni subiti (se inadempimento propri obblighi diretti o violazione delle istruzioni legittime del titolare) e **responsabilità solidale** con il titolare (Art.82)



## 6.2 Contratti con i fornitori



Titolare



Responsabile

Clausole **obbligatorie** da inserire nei contratti/atti di nomina del responsabile:

- ✓ Descrizione dettagliata dei trattamenti: oggetto, durata, natura e finalità dei trattamenti, tipologia di dati registrati, categorie di interessati, obblighi e diritti del titolare
- ✓ Obbligazioni del Responsabile, tra cui:
  - Elenco delle misure tecniche e organizzative
  - Trattamento dei dati solo su istruzioni documentate per iscritto del Titolare, incluse eventuali previsioni sul trasferimento dei dati fuori dalla Unione Europea e obbligo di identificazione del luogo in cui i dati saranno conservati)
  - Obblighi di confidenzialità per il personale del Responsabile
  - Obbligo nel gestire i diritti degli interessati: accesso, correzione, cancellazione, limitazione, opposizione, portabilità
  - Restituzione o cancellazione dei dati a discrezione del Titolare alla cessazione del contratto
  - Obblighi di cooperazione con il Titolare nel notificare i data breach e implementare le valutazioni d'impatto
  - Garantire il diritto di audit e assoggettarsi ad esso
- ✓ Subappalto e Sub-processing: solo con il previo consenso del Titolare e trasposizione obblighi nel contratto con il subappaltatore (responsabilità resta sul Responsabile)

## 7. Trasferimento

- Decisione di adeguatezza (riesame periodico almeno ogni 4 anni + revoca irretroattiva)  
Per le **pubbliche amministrazioni**, in mancanza di una decisione di adeguatezza delle autorità di controllo, possono costituire garanzie adeguate anche le **disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati** (Art. 46)
- Garanzie adeguate (es. Clausole Contrattuali Tipo/SCCs, ma anche codici di condotta o meccanismi di certificazione, se approvati)
- Norme Vincolanti d'Impresa (BCRs: titolari - responsabili)
- Deroghe in specifiche situazioni (es. consenso informato, esecuzione di un contratto, interesse pubblico ecc., ma anche deroghe eccezionali se singoli episodi di trasferimento in determinate circostanze)



## 8. Sanzioni



- Sanzioni **penali** quando previste dalla legge nazionale
- Sanzioni **pecuniarie**: saranno Efficaci, Proporzionate e Dissuasive

fino a **€ 10 milioni**  
o al **2%** del fatturato  
mondiale (se superiore)

- Es. Violazione obblighi in materia di consenso dei minori, misure di sicurezza
- Es. Violazione obblighi impartiti dal Titolare
- Es. Violazione obblighi di comunicazione per Data Breach

Fino a **€ 20 milioni**  
o al **4%** del fatturato  
mondiale (se superiore)

- Es. Violazioni concernenti i diritti degli interessati, i principi cardine del trattamento (es. consenso) i trasferimenti ecc.
- Es. Violazioni di ordini o misure imposte dall'Autorità

Come organizzarsi & Bird & Bird

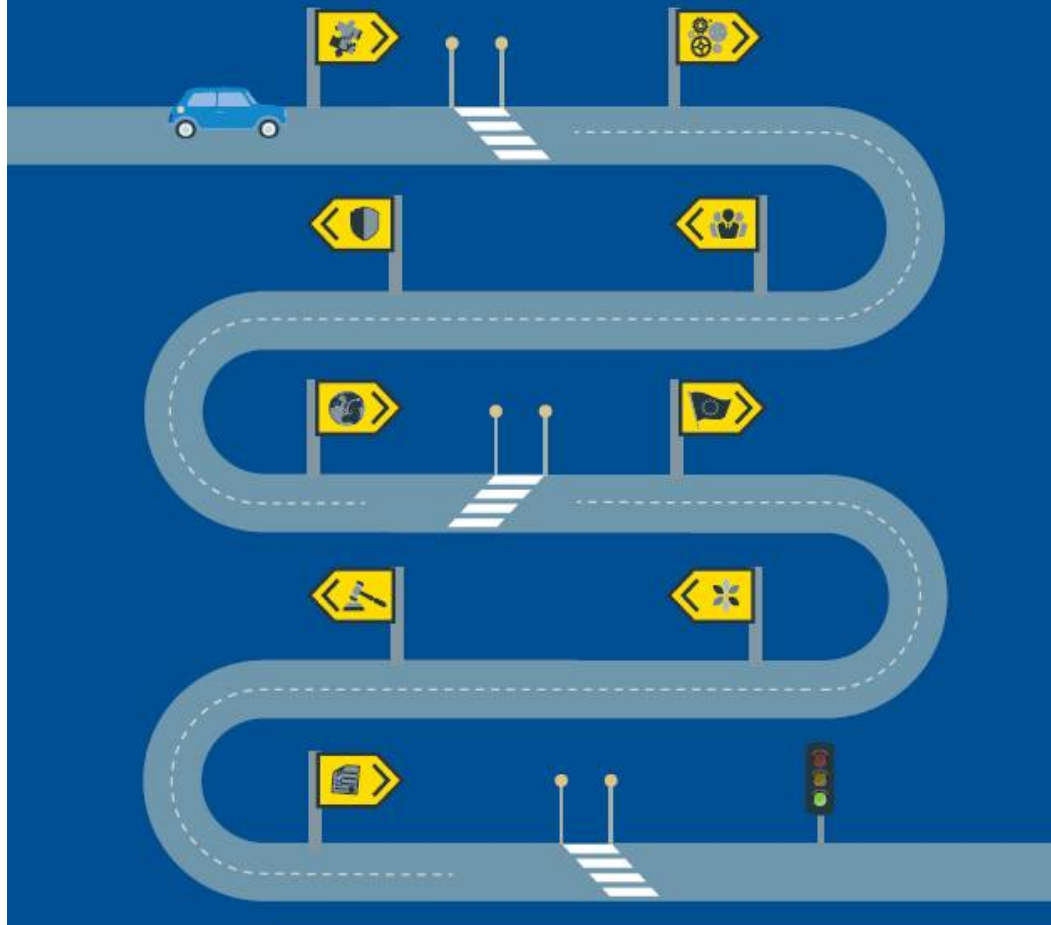


# Prepararsi al Regolamento

1. **Consapevolezza** del cambiamento → analizzare e anticipare gli impatti del Regolamento (analisi dei rischi).
2. **Individuazione dei trattamenti** occorre documentare tutti i trattamenti di dati personali effettuati dall'azienda, precisando per ciascuno di essi l'origine e la natura dei dati, le categorie di interessati, le modalità e le finalità di trattamento, i tempi di conservazione, nonché eventuali comunicazioni a soggetti terzi o diffusioni. → Registro dei trattamenti → censimento.
3. **Revisione della documentazione privacy** → identificare e aggiornare le informative agli interessati, i moduli di consenso, le nomine a responsabile del trattamento e le clausole “Dati Personali” nei contratti con i fornitori o dipendenti e pianificarne l'adozione.
4. **Accountability** → definire un piano di *compliance*, che comprenda le valutazioni di impatto, la revisione dei piani di audit, delle procedure e delle policy nonché piani di formazione.
5. **Privacy by Design & Data Protection Impact Assessment** → iniziare a familiarizzare con questi concetti e capire quando e come implementarli.
6. **Nomina di un DPO.**
7. **Revisione dei presupposti legali** su cui si fondano i trattamenti. Occorre individuare per ciascun trattamento i presupposti legali posti a fondamento dello stesso e registrarli
8. **Data Breaches** → definire le procedure per la rilevazione, segnalazione e indagine di violazioni di sicurezza (entro 72 ore dalla conoscenza dell'evento). Valutare l'adozione di procedure di pseudonimizzazione dei dati e uso della crittografia.

# Bird & Bird & guide to the General Data Protection Regulation

February 2016



<http://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.p>

© Bird & Bird 2016

Cloud e PA –  
Panorama europeo & Bird & Bird

## Analisi comparativa

- I risultati mostrano che sia la Comunità Europea che le autorità nazionali hanno interesse nel Cloud per esigenze amministrative. Tuttavia, anche se le istituzioni UE hanno adottato una strategia per l'adozione dell' *E-Government*, le iniziative nazionali non stanno evolvendo allo stesso ritmo, e che in ogni caso la distribuzione del Cloud nel settore pubblico è ancora alquanto frastagliata.
- A livello nazionale infatti, risulta che alcuni paesi hanno una strategia di cloud in posizione molto avanzata, pur non avendo implementato una "*Government Cloud*" (o "G-cloud"), mentre altri stati hanno predisposto alcune iniziative di Cloud pubblico, senza tuttavia avere una chiara strategia in atto, e, infine, alcuni paesi non hanno alcun G-cloud o strategia in atto, ma hanno comunque mostrato un certo interesse per il cloud computing per l'uso governativo.

## FINLANDIA



- Diversi servizi pubblici sono basati su Cloud. Questa tendenza è destinata ad aumentare in futuro.
- Soluzioni cloud sono comprese nel programma "SADe" del governo coordinato dal Ministero delle Finanze e che mira a sviluppare servizi completi e interoperabili per i cittadini, le imprese e le autorità pubbliche, nonché di migliorare la qualità e l'economicità nel settore pubblico.
- Il programma SADe è collegato con le principali misure di sviluppo delle PA statali e municipali, come ad esempio i programmi per l'efficacia e la produttività degli uffici pubblici, il programma di produttività comunale, e il progetto di sviluppo del servizio clienti del settore pubblico.

## FRANCIA



- Il governo francese ha mostrato interesse nelle soluzioni Cloud, e sta cercando di sviluppare un servizio Cloud da mettere a disposizione delle amministrazioni e delle aziende francesi. Tale servizio sarà incentrato sulla conservazione dei dati sensibili, come i dati sanitari, i dati amministrativi e i dati economici che richiedono la massima sicurezza.
- A seguito dell'invito a manifestare interesse del governo francese, due proposte sono state selezionate per lo sviluppo del progetto "Andromède": Thales/Orange (cloudwatt) e Sfr/Bull (Numergy).

## BELGIO



- Il governo federale belga e le entità federate hanno mostrato interesse verso le soluzioni cloud per le proprie istituzioni e i servizi amministrativi.
- Dal marzo 2015 è operativo un "Government Cloud" (o G-Cloud). Il G-Cloud è il risultato di una iniziativa congiunta tra diversi istituzioni pubbliche. Fornisce una infrastruttura IT sulla quale le PA locali possono installare i propri applicativi e le proprie Banche Dati.
- I primi servizi disponibili includono lo "Storage as a Service" e "Infrastructure as a Service". Il programma G-Cloud svilupperà in futuro anche servizi del tipo "Platform as a Service" e "Software as a Service".

## SPAGNA



- Gli enti pubblici spagnoli stanno mostrando un crescente interesse verso le soluzioni Cloud.
- Non esiste ancora un "Government Cloud", ma le autorità spagnole hanno stabilito un programma tendente verso un modello di "comunità Cloud" per tutta l'amministrazione pubblica (con l'integrazione di amministrazione nazionale, regionale e locale).
- La diffusione del Cloud computing tra enti del settore pubblico spagnolo è però ancora limitata, ed è più in uso tra le autorità locali di governo centrale o degli organi comunitari autonomi.



## GRAN BRETAGNA



- Il governo centrale sta promuovendo attivamente l'adozione del Cloud negli uffici amministrativi. A tale scopo, l'Ufficio di Gabinetto ha istituito il programma "G-Cloud" attraverso il quale i provider possono fornire i propri servizi agli enti pubblici.
- La maggior parte dei dipartimenti governativi stanno introducendo servizi Cloud nei loro accordi di outsourcing esistenti.
- A livello locale le PA utilizzano già da qualche anno una vasta gamma di servizi Cloud (in particolare le autorità comunali e le scuole).

## GERMANIA



- Le autorità tedesche, in particolare a livello statale (Bundesland) stanno considerando di istituire Cloud di tipo privati per le PA.
- Attualmente si stanno valutando progetti concreti che mirano all'introduzione di Cloud privati nel settore pubblico (ad esempio, a Berlino e in Renania-Palatinato).

Un'analisi comparativa della legislazione vigente in 19 Paesi dell'Unione Europea rilevante a fini del cloud

**Cloud law at your fingertips**

- V4 is 5x faster
- Expert content on cloud law in 19 countries
- Now includes guidance on Safe Harbour and the GDPR

Download on the App Store

ANDROID APP ON Google play

Get it from Microsoft

## In poche parole...

~~Il cloud computing non è compatibile con il trattamento dei dati da parte di una PA ...~~

...SBAGLIATO...

Il cloud computing **PUO' ESSERE** data protection compliant,  
**ANCHE NEL SETTORE PUBBLICO**



Grazie & Bird & Bird

[deborastella@twobirds.com](mailto:deborastella@twobirds.com)