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

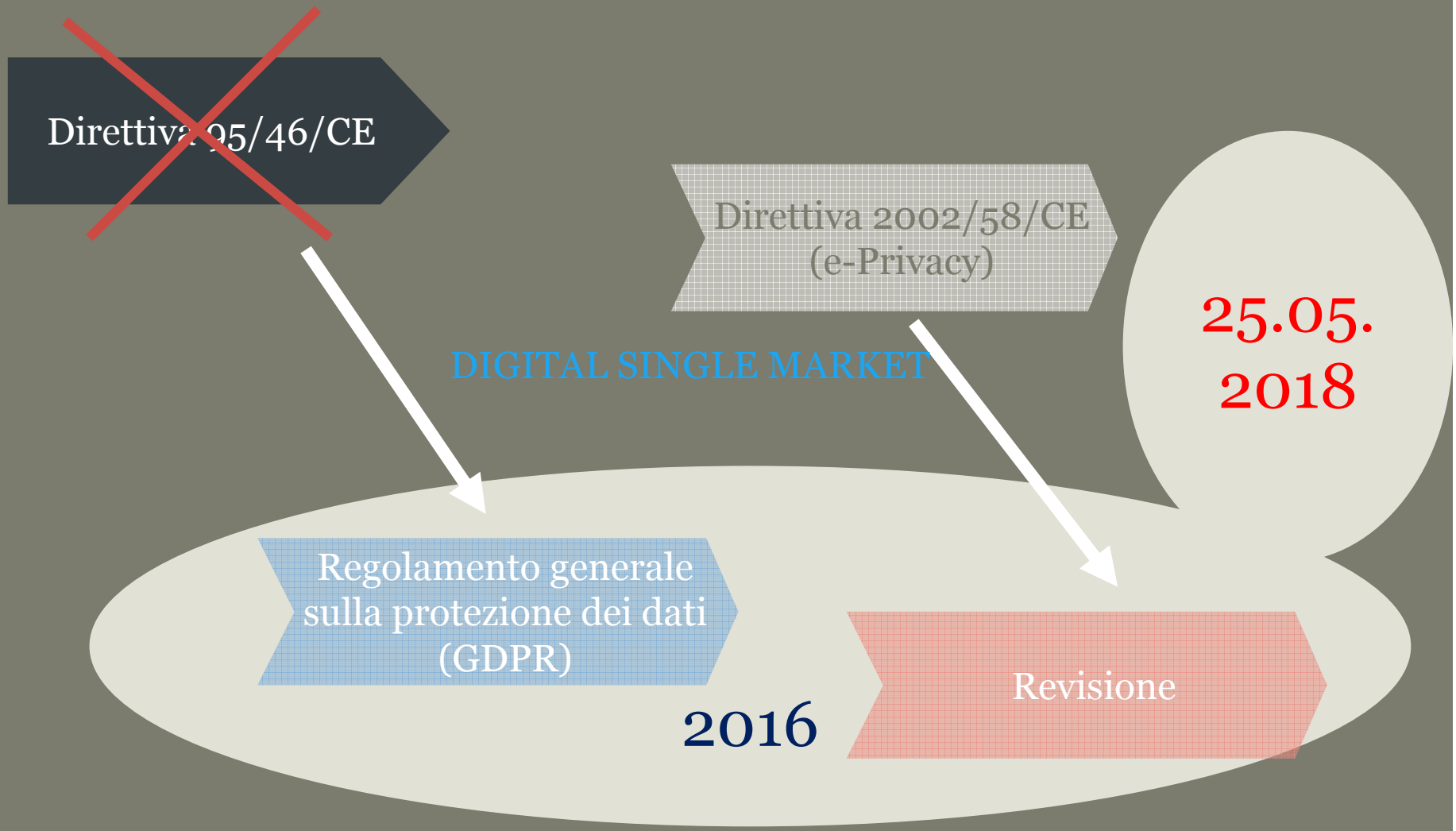
& Bird & Bird

*Roma – 5 ottobre 2016*

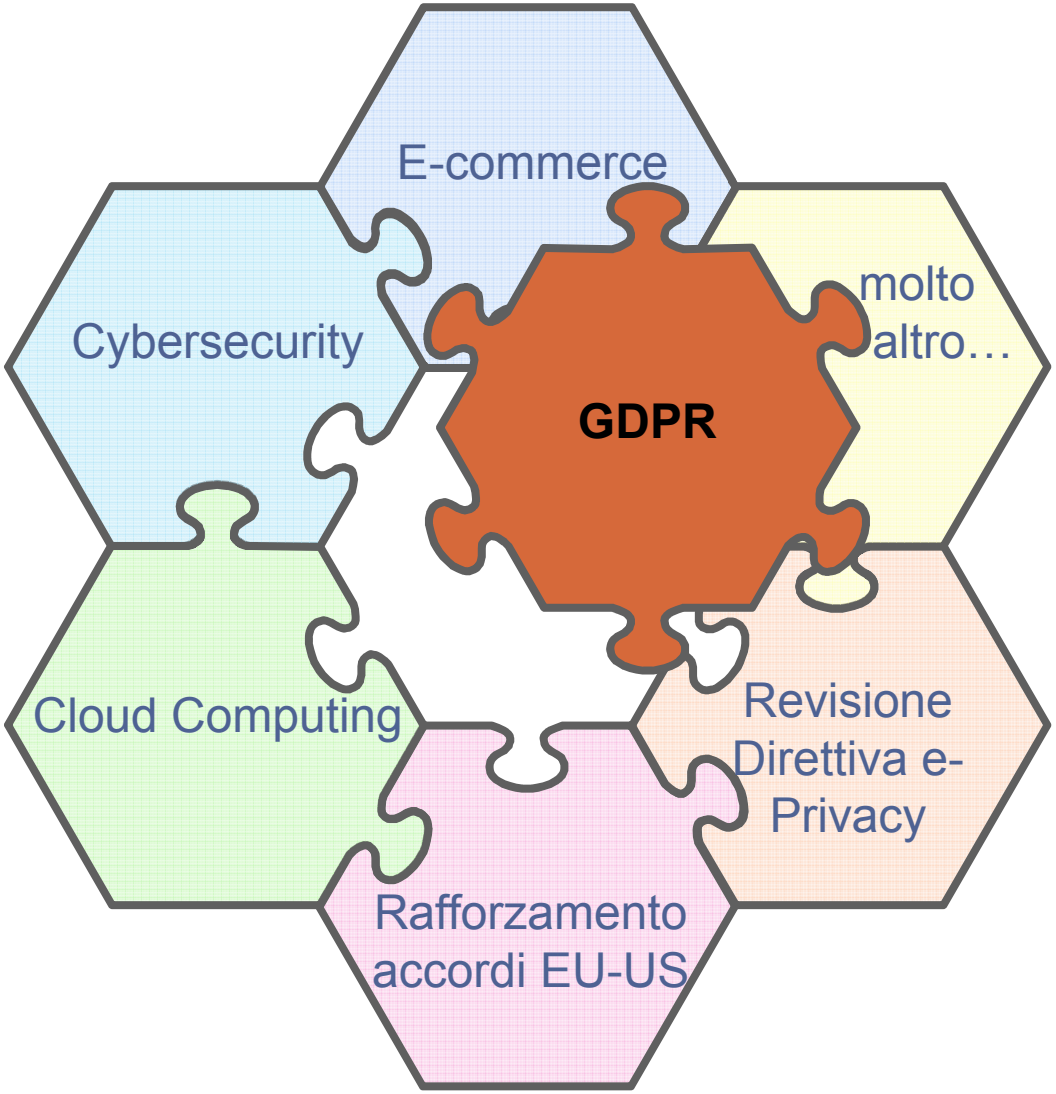
*Avv. Debora Stella*

*Studio Legale Bird & Bird*

# EU: Dalle origini ad oggi



# Tutto al proprio posto…






Bird & Bird

# 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

1. Nuove informazioni

2. Accountability & Dimostrazione della compliance

3. Valutazioni di impatto

4. Nomina di un Data Protection Officer

5. Segnalazione Data Breach

6. Nuovi requisiti per i fornitori

7. Trasferimenti

8. Sanzioni più rigide

•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 portabiità 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 limiazione del trattamento
  - ✓ Diritto alla portabilità dei dati (a certe condizioni)
  - ✓ Diritto di opporsi a processi di trattamento automatizzati

# 2. Accountability al posto delle notifiche

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

A carico di titolari **e responsabili**

## To Do List

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



Bird & Bird

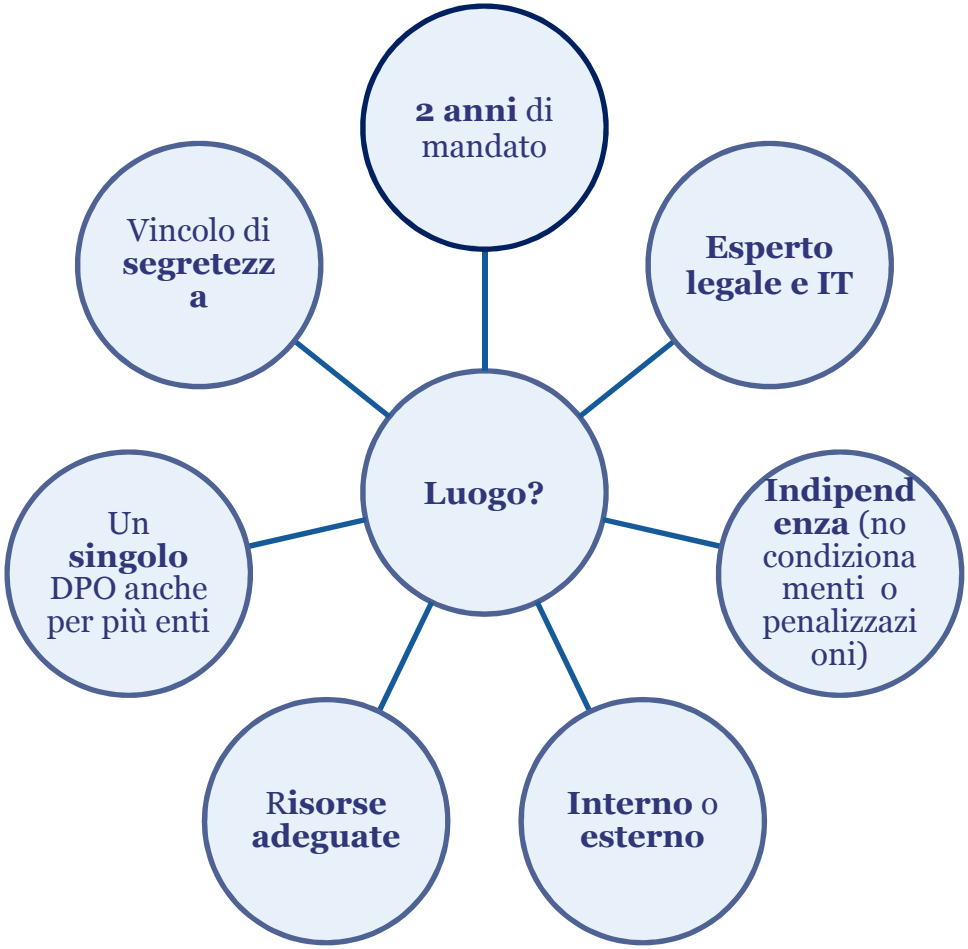
# 3. Valutazioni d'impatto

- 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 dignitò dei cittadini, es.:

| | | | |
|---|---|---|---|
| Trattamento su larga scala di dati sensibili | Attività di profilazione | Sistematica sorveglianza su larga scala di zona accessibile al pubblico | Altri trattamenti previsti dalle autorità di controllo |

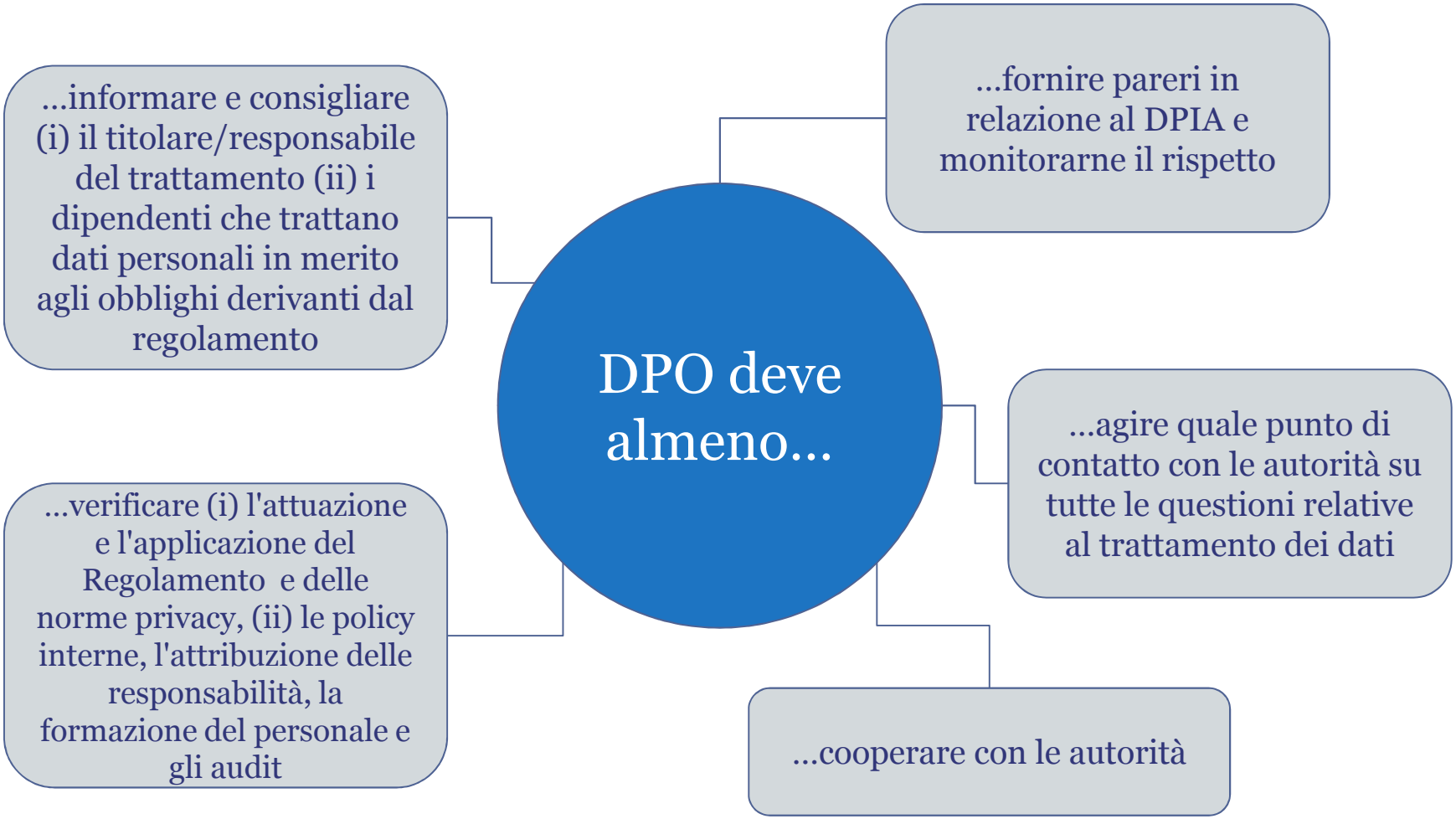
- Contiene almeno:
  - Una descrizione specifica dei trattamenti e delle finalità
  - Una valutazione di proporzionalità del trattamento, dei rischi connessi e delle misure di mitigazione dei rischi (specie misure di sicurezza, garanzie)
- Identificazione delle aree di rischio elevato: definita dalle 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**

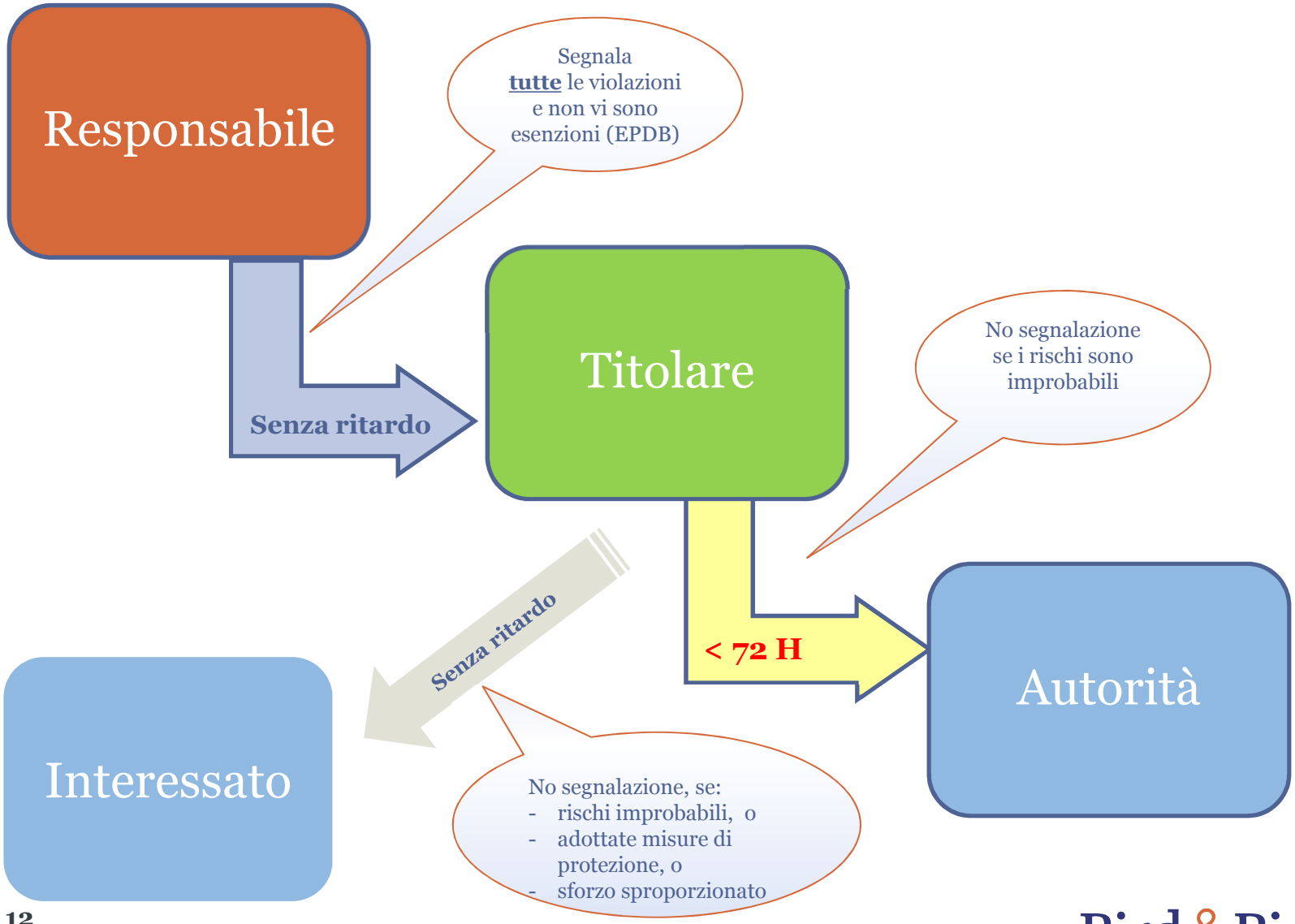
# 4.2. Principali compiti del DPO






Bird & Bird

# 5.1 Segnalazioni di Data Breach






Bird & Bird

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

- 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)

## To Do List

☑ 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 <u>diretti</u> 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 requisti di **sicurezza sui dati** adottando misure specifiche parametrate 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 <u>diretta</u> verso gli interessati per i danni subiti (se inadempimento propri obblighi diretti o violazione delle istruzioni legittime del titolare) e responsabiità <u>solidale</u> con il titoalre (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 regitrati, 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 conil subapaltatore (responsabilità resta sul Resposanbile

# 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 Regoamento (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** → dentificare 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.