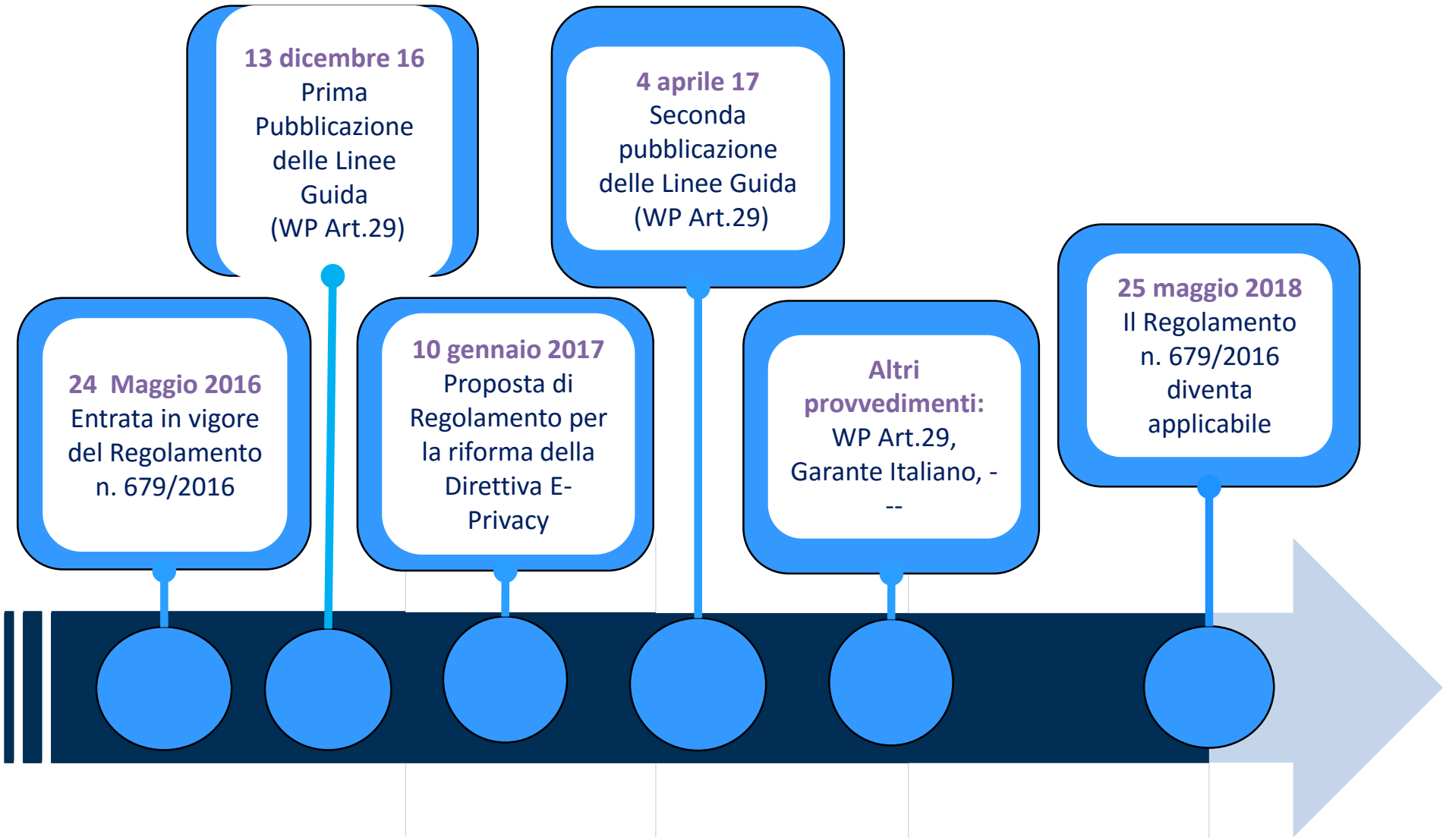
Convegno Annuale AISIS

Privacy e Sicurezza
A supporto dell'innovazione digitale in Sanità

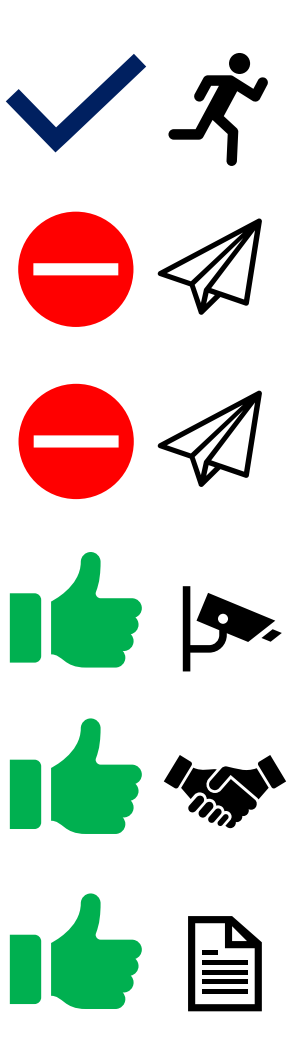
Il GDPR: inquadramento generale e cosa stanno facendo le Aziende

Gabriele Faggioli
Presidente CLUSIT – Osservatorio Sicurezza & Privacy Politecnico di Milano

Torino, 12 e 13 ottobre 2017
Hotel NH Torino Centro

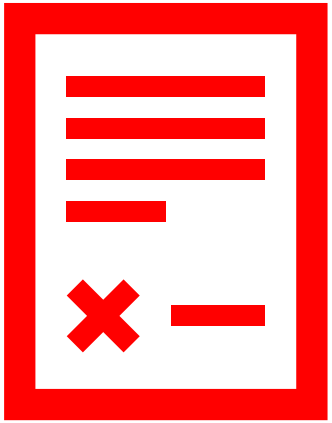

13 dicembre 16
Prima Pubblicazione delle Linee Guida (WP Art.29)
4 aprile 17
Seconda pubblicazione delle Linee Guida (WP Art.29)
24 Maggio 2016
Entrata in vigore del Regolamento n. 679/2016
10 gennaio 2017
Proposta di Regolamento per la riforma della Direttiva E-Privacy
Altri provvedimenti:
WP Art.29, Garante Italiano, ---
25 maggio 2018
Il Regolamento n. 679/2016 diventa applicabile

Regolamento 2016/679	**IN VIGORE, NON APPLICABILE (?)**
Direttiva 1995/46	**IN VIGORE, DECADE il 24 maggio 2018**
Autorizzazioni Generali Autorità Garante	**IN VIGORE, DECADONO il 24 maggio 2018**
Provvedimenti Autorità Garante	**NON DECADONO** fino a quando non verranno modificati, sostituiti, abrogati
Accordi internazionali su trasferimento dati	**NON DECADONO** fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissione UE	**NON DECADONO** fino a quando non verranno modificate, sostituite, abrogate



INVARIATI O VARIATI MARGINALMENTE

- Definizione di trattamento
- Definizione di dato personale
- Principi relativi al trattamento di dati (ma tempo di matenimento da valutare)
- Liceità del trattamento
- Obbligo di informativa
- Obbligo di consenso
- Soggetti che effettuano il trattamento (salvo incaricati e DPO)
- Protezione delle sole persone fisiche



NOVITA' DEL REGOLAMENTO

- Accountability del titolare
- Nuovi diritti degli interessati: portabilità, oblio, conservazione, …
- Registro dei trattamenti
- Responsabilità solidale di titolare e responsabile
- Sicurezza basata su analisi dei rischi e adozione di misure tecniche e organizzative adeguate
- Obbligo di notifica dei Data breach
- Data protection by design e by default
- Valutazione d'impatto e consultazione preventiva
- Data Protection Officer (DPO)
- Certificazione dei trattamenti
- Entità delle sanzioni

Sono stati individuati **4 cantieri di lavoro**, suddivisi a loro volta in **21 sottocantieri** di cui si evidenzia l'eventuale relazione con i requisiti del Regolamento

LEGALE

- Registro dei trattamenti — GDPR
- Fornitori e Contratti — GDPR
- Informative, consensi e moduli raccolta dati — GDPR
- Diritti degli interessati — GDPR
- Lettere di nomina
- Data Protection Impact Assessment — GDPR
- Privacy By Design / Privacy By Default — GDPR
- Trasferimento dati estero — GDPR

ORGANIZZAZIONE E RISORSE UMANE

- Organizzazione e risorse — GDPR
- Comunicazione, formazione e affiancamento
- Investimenti
- Program Management Officer (PMO)

SISTEMI INFORMATIVI

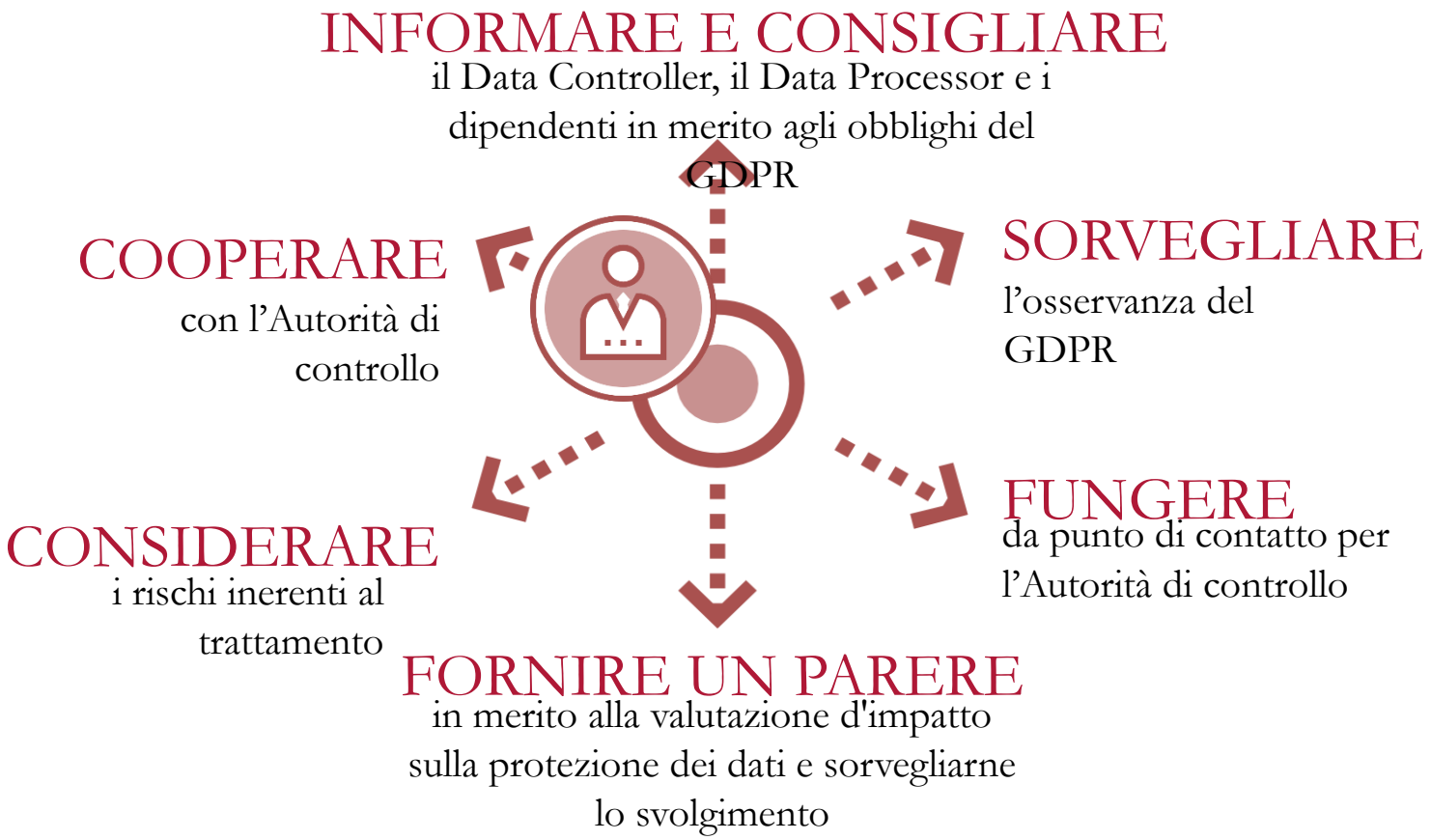
- Valutazione rischi IT — GDPR
- Misure di sicurezza IT — GDPR
- Data breach — GDPR
- Applicativi, Dati e Infrastrutture
- Piattaforma GRC

COMPLIANCE

- Accountability — GDPR
- Valutazione rischi non conformità
- Sistema di controllo interno

IMPIANTO DOCUMENTALE

Il GDPR ha introdotto anche la nuova figura del Data Protection Officer (c.d. DPO) che la funzioni di:



Il DPO deve…

INDIPENDENZA
Nell'esercizio delle sue funzioni

COMPETENZE
giuridiche, informatiche, di risk management e di analisi dei processi

INTERFACCIARSI
Con le figure chiave dell'azienda

Il WP29 nelle «*Linee-guida sui responsabili della protezione dei dati*» (WP243) ha individuato una serie di ipotesi in cui la figura del DPO potrebbe essere in conflitto d'interesse.

1. Ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT);
2. posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento;
3. inoltre, può insorgere un conflitto di interessi se, per esempio, a un DPO esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

Il DPO è obbligatorio quando…

Il trattamento sia effettuato da un'**autorità pubblica**

Il "core business" dell'azienda consista nel trattamento "**su larga scala**" **di dati "sensibili" e "giudiziari".**

Il "core business" dell'azienda consista in attività che richiedono il **monitoraggio regolare e sistematico di dati "su larga scala".**

Le ipotesi di obbligatorietà della nomina del DPO sono state specificate dall'"*Article 29 Data Protection Working Party*" (di seguito, "**WP29**"), con le Linee Guida sul DPO adottate il 13 dicembre 2016, emendate e revisionate il 5 aprile 2017 (WP243).

Le responsabilità nel GDPR….

Responsabilità del titolare (Accountability)
Art. 24

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche il **titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente alla legge.

Responsabilità di titolare e responsabile
Art. 82 c. 2

Un **titolare** del trattamento coinvolto nel trattamento **risponde** per il **danno** cagionato dal suo trattamento che **violi il presente regolamento**.

Un **responsabile** del trattamento risponde per il danno causato dal trattamento **solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili** del trattamento **o** ha **agito in modo difforme o contrario rispetto alle** legittime **istruzioni del titolare** del trattamento.

Responsabilità solidale di titolari e responsabili
Art. 82 c. 4

Qualora **più titolari del trattamento o responsabili** del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano **coinvolti nello stesso trattamento** e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, **ogni titolare del trattamento o responsabile del trattamento è responsabile in solido** per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Responsabilità dei contitolari
Art. 26

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**.

Grazie dell'attenzione e buon lavoro