Il nuovo Regolamento europeo sulla protezione dei dati e il suo impatto specie in ambito sanitario

Milano 9 novembre 2017

Chiara Romano

Un «pacchetto» non isolato…

- Regolamento (UE) 2016/679 sulla protezione dei dati;
- Direttiva (UE) 2016/680 polizia e giustizia

…ma accompagnato dalla revisione di altri rilevanti strumenti sovranazionali in materia:

- Proposta di Regolamento sulla vita privata e le comunicazioni elettroniche ("Regolamento ePrivacy")

Il mutamento di prospettiva è la vera rivoluzione

- **Focalizzato sui diritti degli interessati** (supera la dimensione riduttiva del mercato interno)
- **La sua applicazione supera i confini nazionali ed europei** (dimensione digitale è refrattaria ai criteri della nazionalità e della residenza: principio del targeting)
- **Livello di tutela uniforme e coerenza nell'applicazione delle regole** (supera le asimmetrie delle legislazioni nazionali, meccanismo dello sportello unico e meccanismo di coerenza, cooperazione tra DPA e ruolo del CEPD, sistema sanzionatorio europeo)

Il mutamento di prospettiva è la vera rivoluzione

- **Tutela proattiva e preventiva, meno reattiva difensiva, riparatoria e burocratica** (valutazione del rischio-PIA, notifica *data breach, privacy by design* e *privacy by default,* pseudonimizzazione)
- **Responsabilizzazione** (DPO, registro dei trattamenti, certificazioni di conformità, adesione a codici di condotta)
- **Vincolatività e diretta azionabilità dei principi generali del trattamento** (responsabilizzazione, liceità, trasparenza, limitazione della finalità minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, requisiti di validità del consenso)

Altre novità in pillole

- **Nuovi diritti per gli interessati: limitazione del trattamento, diritto alla portabilità, diritto all'«oblio»**
- **Nuove modalità semplificate per l'informativa (tramite l'utilizzo di icone)**
- **Particolare attenzione ai minori**
- **Ruolo delle associazioni dei consumatori o per la tutela di interessi collettivi (*class action*)**
- **Consultazione obbligatoria della DPA anche sugli schemi di atti legislativi**

Impatto nell'ordinamento nazionale

- Regolamento → armonizzazione
- Normativa statale → completamento
- Atti della Commissione → coerenza nell'attuazione (es. criteri e i requisiti comuni dei meccanismi di certificazione e norme tecniche)

Il legislatore nazionale è tenuto a:

- Emanare norme di «attuazione»: es. criteri per le certificazioni e per l'accreditamento degli organismi di certificazione, previsione di eventuali ulteriori sanzioni amministrative o anche penali, norme sull'istituzione, le risorse e il funzionamento dell'Autorità di controllo…

Impatto nell'ordinamento nazionale

Ma ha qualche margine di discrezionalità → «flessibilità»:

- Mantenere o introdurre disposizioni «più specifiche»: per i trattamenti svolti in ottemperanza a obblighi di legge o per l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri o per adeguare le norme di Regolamento a interi settori che richiedono disposizioni più specifiche (es. ricerca scientifica o storica, trattamenti a fini statistici, archivi di interesse pubblico, accesso a documenti, rapporti di lavoro, giornalismo, chiese e associazioni religiose)
- Mantenere o introdurre ulteriori condizioni: con riguardo al trattamento di «dati sensibili» (dati genetici, biometrici, o relativi alla salute)

Impatto nell'ordinamento nazionale

Ma con qualche margine di manovra:

- Integrazione normativa (facoltativa): età per validità del consenso dei minori in rapporto ai servizi della società dell'informazione, ulteriori casi di designazione obbligatoria di DPO, autorizzazione preventiva della DPA per trattamenti svolti nel pubblico interesse, compresi quelli a fini di sanità pubblica, poteri ulteriori della DPA (accesso civico, cyberbullismo, telemarketing) sanzioni amministrative per i soggetti pubblici, ecc.
- Introdurre deroghe: ai diritti degli interessati sulla base di preminenti interessi pubblici generali, o nel campo della ricerca scientifica o storica, dei trattamenti a fini statistici o per finalità di archiviazione nel pubblico interesse

Impatto nell'ordinamento nazionale

Legge di Delegazione Europea 2016-2017 (l. 25 ottobre 2017, n. 163) Art. 13

uno o più decreti legislativi

previo parere delle commissioni parlamentari e del Garante

- abrogare espressamente le disposizioni del Codice incompatibili con le disposizioni del GDPR;
- modificare il Codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel GDPR;
- prevedere il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante;
- adeguare, nell'ambito delle modifiche al Codice, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del GDPR con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

Cosa cambia? Per tutti:

- Campo di applicazione (si applica ai trattamenti non automatizzati di dati se contenuti o destinati ad archivi, non si applica ai deceduti, spariscono i dati anonimi, se ne prevede l'applicazione anche a soggetti stabiliti extra-UE)
- Figure e ruoli (non sono più contemplati gli incaricati e i responsabili interni, obblighi specifici per il responsabile esterno, possibilità di ricorrere a sub-responsabili, più trasparenza per i contitolari, DPO)
- Adempimenti (non più prevista la notificazione e l'obbligo di verifica preliminare, ma PIA con eventuale consultazione preventiva della DPA, estensione obbligo data breach, registro delle attività di trattamento)

Cosa cambia? Per tutti:

- **Dicotomia soggetti pubblici/privati** (ma possibili specificazioni per trattamenti svolti nel pubblico interesse o connessi all'esercizio di pubblici poteri o per adeguare le norme GDPR a specifici settori)
- **Codici deontologici** (non più condizione di liceità del trattamento, possibilità di mantenerli nei settori in cui è consentito agli SM mantenere o introdurre disposizioni più specifiche, es. ricerca scientifica, storica, statistica, archivi di interesse pubblico)
- **Misure “minime” di sicurezza** (adeguate al rischio)
- **Tutela dinanzi al Garante** (unica forma di tutela per l’interessato)
- **Sanzioni amministrative** (tassative, vanno fissati i minimi edittali, ma possibili margini di flessibilità, ne bis in idem)

Cosa cambia?
Ambito sanitario

- «Dati relativi alla salute» (art. 4.1(15) +cons. 35)
- «Dati genetici» (art. 4.1(13) + Cons. 34)
- Presupposti di liceità (art. 9.2)
  - Specifici criteri di legittimazione per i trattamenti in ambito sanitario → residualità del consenso «esplicito» vs. «scritto» → compatibilità vigenti previsioni su modalità semplificate per la manifestazione del consenso

Cosa cambia? Ambito sanitario

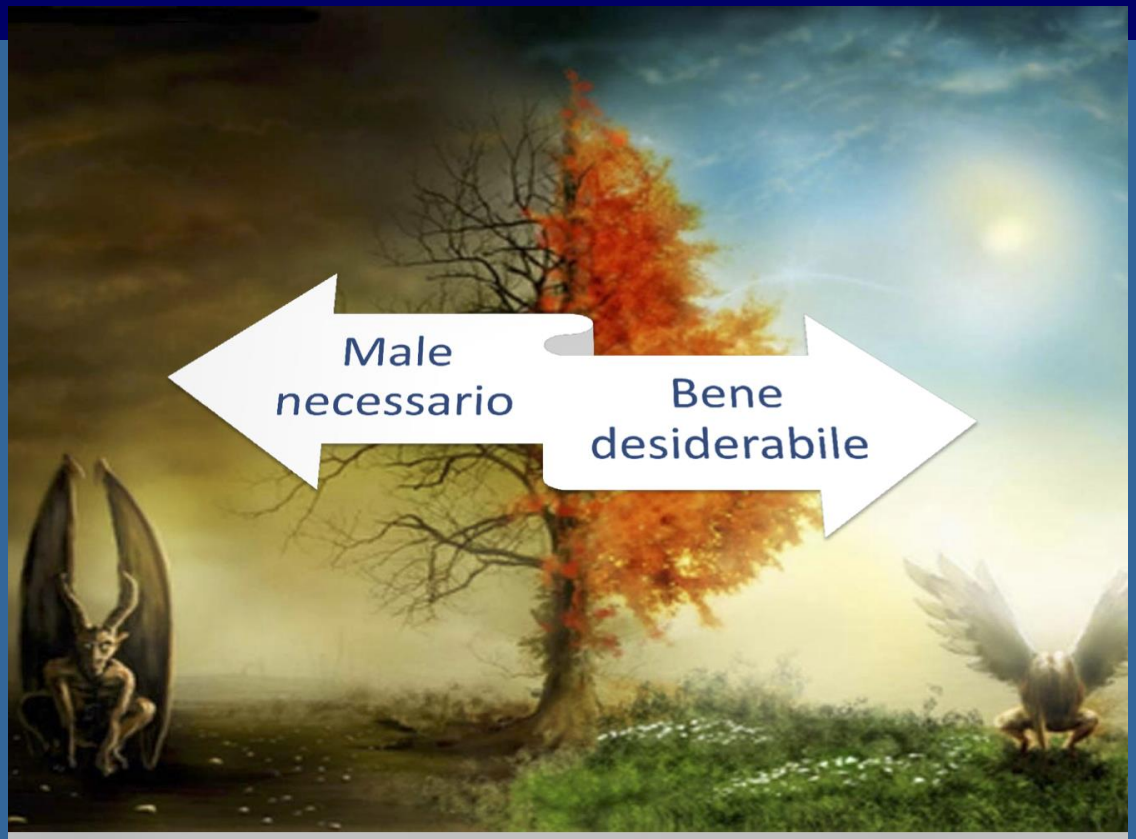
- Presupposti di liceità (art. 9.2)
  - (a): consenso esplicito
  - (c): tutela interessi vitali interessato o terzi
  - (h): necessario per medicina preventiva o occupazionale, diagnosi, servizi sanitari, gestione sanitaria → sulla base del diritto nazionale + a cura di un professionista della sanità (9.3)
  - (i): interesse pubblico (nel settore sanità pubblica) → sulla base del diritto nazionale/Reg. 1338/2008 sulle statistiche comunitarie in materia sanitaria

Cosa (non) cambia?

- **Margine di flessibilità per Stati Membri (rinvio a diritto nazionale):**
  - **Art. 6.2: rinvio generale al legislatore nazionale (trattamenti in adempimento obblighi di legge e per «interesse pubblico» → possibilità di introdurre «adattamenti» alle disposizioni Regolamento alle CONDIZIONI di cui all'art. 6.3)**
  - **Art. 9(5): Possibilità di introdurre «condizioni o requisiti ulteriori» (anche limitazioni) per trattamenti dati genetici, biometrici, di salute**
  - **Art. 36.5: (PIA) Possibile obbligo consultazione ed eventuale autorizzazione DPA per trattamenti nel pubblico interesse, compresa sanità pubblica**

Diposizioni del Codice per l'ambito sanitario, autorizzazioni generali e linee guida del Garante, regolamenti dati sensibili, Coc…

Cosa è indispensabile?



Un passo avanti

Cosa è indispensabile?

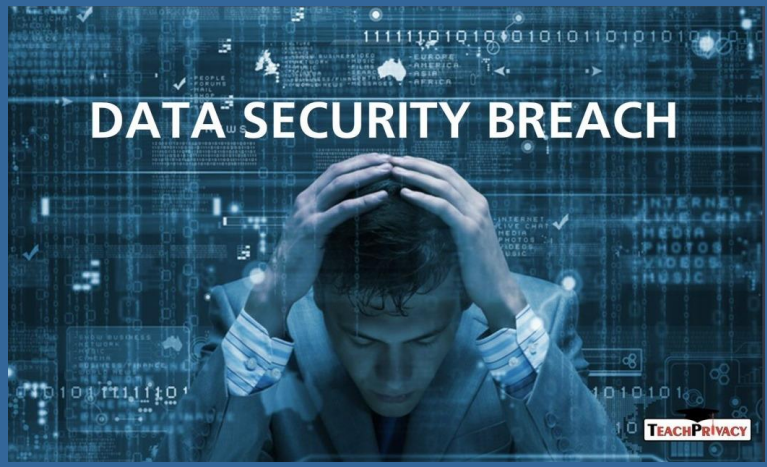
- **Mutamento culturale da parte di amministrazioni, imprese, individui**
- **Privacy: risorsa strategica di sviluppo e di sicurezza generale del Paese**

→fattore di competitività e non mero obbligo burocratico

Cosa resta da fare?

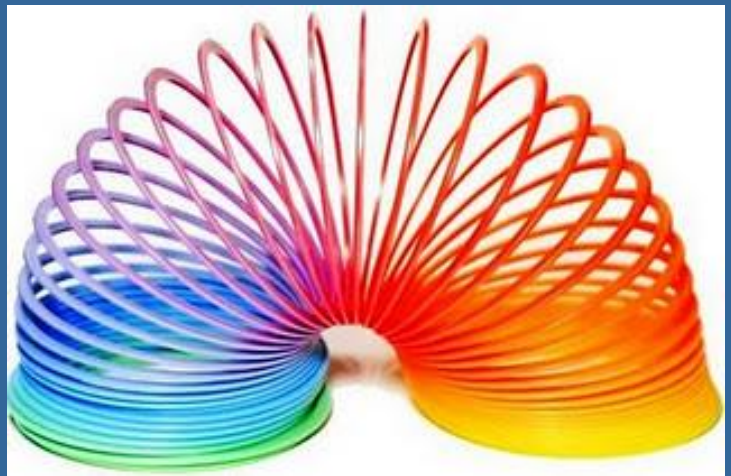
- Sondaggio (340 dirigenti aziendali a livello globale)
- 45% delle organizzazioni intervistate ha un piano strutturato per adeguarsi al nuovo GDPR
- Tra queste solo il 66% ritiene che il processo sarà in grado di soddisfare i requisiti di conformità
- 58% non è del tutto consapevole delle conseguenze derivanti dal mancato adeguamento

Dotarsi di una solida strategia di Governance dei dati



SURSUM CORDA

- **Fase di transizione: difficile, ma non impossibile**
- **Opportunità di valorizzare le esperienze esistenti e modificare quelle fallimentari (settore sanitario)**
- **Opportunità per razionalizzare e migliorare**



Grazie per l’attenzione

c.romano@gpdp.it

www.garanteprivacy.it

… e Auguri!