Regolamento Europeo 2016/679 del 27.4.2016
Protezione delle persone fisiche con riguardo al trattamento dei dati personali

Definizione di un «Codice di Condotta» per la sanità

Fabrizio Massimo Ferrara

Roma, 4 Aprile 2018

Il regolamento

Il regolamento costituisce un quadro di riferimento completo ed organico di principi e di regole, innanzi tutto di natura metodologica ed organizzativa

NON è una check-list

Nel rispetto dei principi generali definiti nel regolamento

le singole organizzazioni devono definire, implementare e gestire un proprio sistema organico di

- strutture organizzative
- procedure operative
- soluzioni tecniche
- documentazione

per la gestione, la sicurezza e la protezione dei dati personali

Criticità

- **I principi sanciti dal GDPR sono necessariamente di validità generale** ed indipendenti dalle specifiche caratteristiche ed esigenze dei diversi domini di attività.

- **Onere dell'organizzazione, innanzi tutto, è quindi la definizione di un insieme di regole, che declinino i principi generali del GDPR secondo le caratteristiche e le esigenze del particolare dominio di attività** (es. sanità, banca, e-commerce, etc.). La rispondenza di queste regole ai principi del GDPR è elemento qualificante anche nell'ambito degli eventuali procedimenti di responsabilità e sanzionatori.

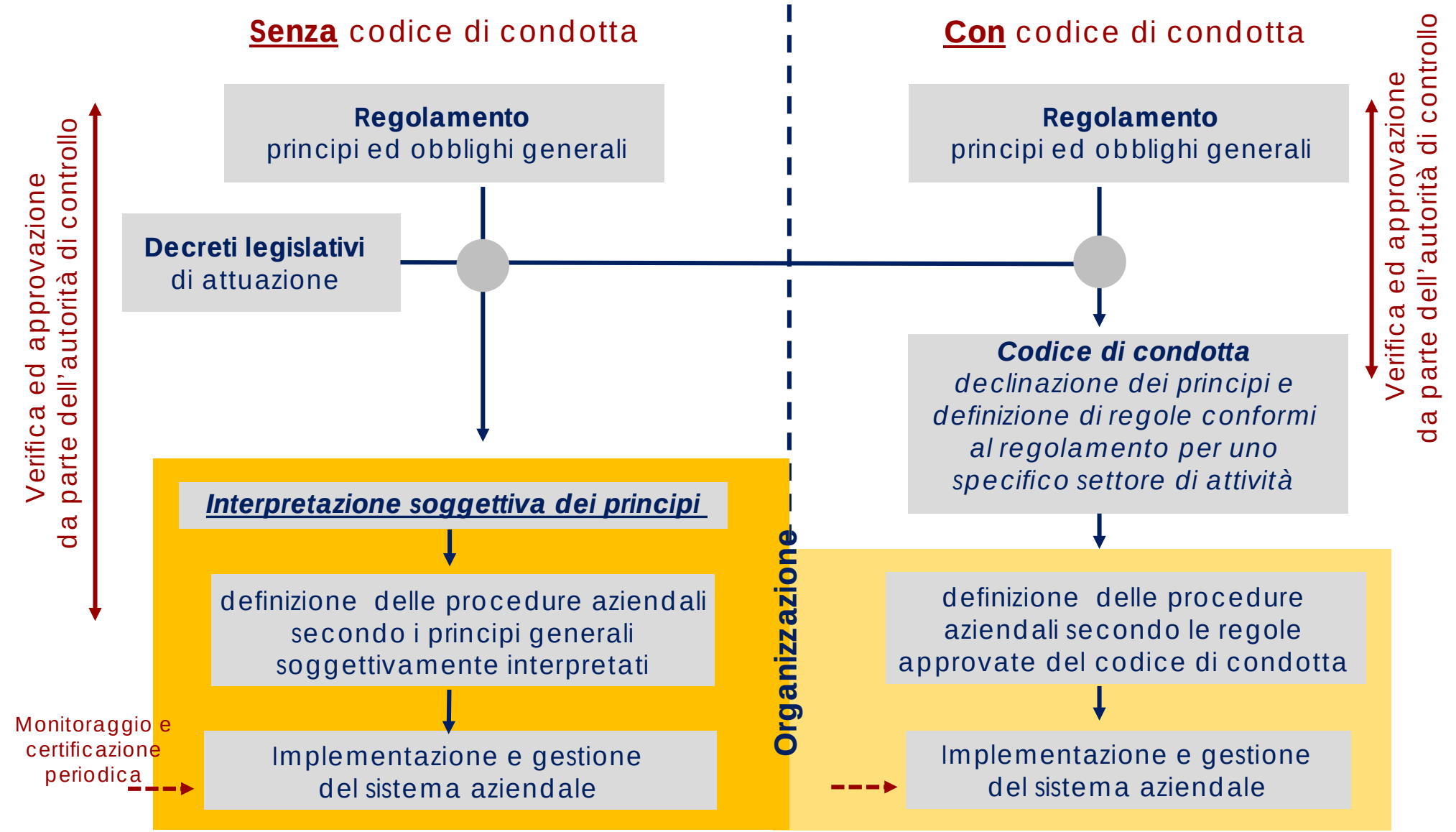
- **Sulla base di queste regole, dovrà poi essere definito, implementato e manutenuto il sistema di protezione e controllo specifico** della organizzazione stessa (art. 24).

I Codici di condotta

- Per facilitare l'individuazione delle modalità secondo cui declinare i principi generali nel proprio settore di attività, è prevista la definizione dei cosiddetti "**Codici di condotta**" (art. 40).

- Un "**codice di condotta**" costituisce un insieme di regole che dettagliano le modalità di attuazione e la corretta applicazione del regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle diverse tipologie di organizzazioni.

Onere dell'organizzazione



Rispetto ad altri settori, il contesto sanitario è caratterizzato da un insieme di strutture

- **peculiari** per la loro attività e la loro missione etica e sociale
- **diverse** sotto il profilo organizzativo, clinico, dimensionale, tecnologico
- **autonome** sotto il profilo organizzativo, sanitario e giuridico

ma con necessità di interagire e cooperare fra loro nella cura del paziente

Elementi qualificanti per la validità/usabilità del codice

(oltre ovviamente al rispetto del Regolamento)

- **Aderenza delle regole alle reali esigenze** e specificità del contesto sanitario
- **Uso di un modello di validità generale** per definire regole omogenee applicabili nei diversi scenari organizzativi e tecnologici, anche interconnessi
- **Validazione e consenso** il più ampio possibile da parte delle diverse realtà

L'iniziativa

Istituzioni ed associazioni sanitarie e professionali di rilevanza nazionale.

- AIOP – Associazione Italiana ospedalità privata
- ARIS – Associazione Religiosa istituti socio sanitari
- FederANISAP - Federazione Nazionale delle Istituzioni Sanitarie Ambulatoriali Private
- Federsanità-ANCI
- FIASO – Federazione italiana aziende sanitarie e ospedaliere
- Ministero della Salute - Direzione generale della vigilanza sugli enti e della sicurezza della cure
- Ordine dei medici della provincia di Roma, *anche per la validazione clinica della liceità e finalità del trattamento*

Organizzazioni sanitarie, direttamente coinvolte anche per la verifica della applicabilità di quanto previsto nei contesti reali

- ASL di Foggia
- ASL Roma-1
- Azienda di Tutela della Salute Val Padana
- Azienda Unità Sanitaria Locale della Romagna
- Azienda USL Toscana sud est

Cittadini, intesi sia come proprietari dei dati, sia come interlocutori attivi e continui nel processo sanitario.

- Cittadinanzattiva

Organizzazione

Core Team

Coinvolgimento attivo, pianificato e continuo per:
- Coordinamento e pianificazione delle attività
- Definizione delle metodologie e delle linee di indirizzo
- Redazione dei documenti sulla base dei contributi, con una metodologia scientifica di analisi del consenso.

Extended Team – Referenti delle aziende ed associazioni partecipanti

Partecipazione secondo le disponibilità individuali, pianificata nelle singole attività
- Contributi e revisione generale dei documenti di lavoro
- Approfondimenti specifici mediante gruppi di lavoro ad-hoc
- Diffusione e validazione nell'ambito della propria associazione

Forum – Associazioni, organizzazioni, aziende interessate a contribuire

Contributo volontario estemporaneo
- Commenti e contributi sui documenti intermedi pubblicati

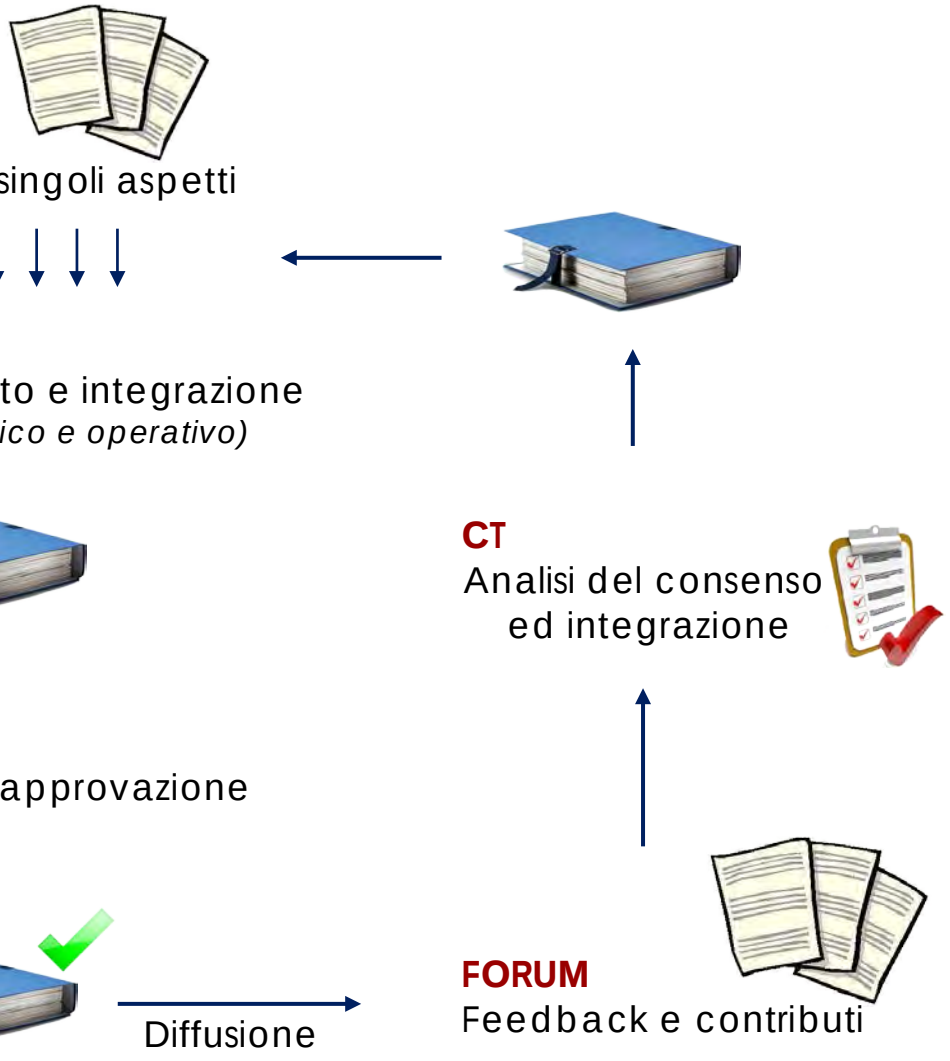
Metodo di lavoro e definizione del consenso

Una stretta collaborazione fra core team ed extended team

e verifica/ raffinamento incrementale con una platea più ampia

<u>secondo tecniche basate sul «consensus method»</u>

in modo da assicurare la convergenza e sinergia dei diversi contributi



Metodologia per la definizione del codice

GDPR
Principi generali validi per tutti

Decreti legislativi
di attuazione

Contesto sanitario

Aspetti normativi
- Legislazione
- Linee di indirizzo

Modello di riferimento
Indipendente da struttura organizzativa e tecnologica
- Processi (trattamenti)
- Esigenze
- Scenari operativi

Ambito dell' iniziativa

Codice di condotta
Regole di riferimento per il settore sanitario

Singola azienda

Descrizione del proprio contesto e correlazione con il modello

Sistema, procedure e soluzioni specifiche della azienda

Usabilità del codice di condotta

Il Regolamento deve rappresentare **un'opportunità di miglioramento**, non solo un obbligo formale

Per facilitare l'usabilità del codice, sono previste due tipologie di sezioni

Sezioni di **carattere normativo**

contenenti la **specifica delle regole (organizzative e tecniche)** da applicarsi puntualmente nei singoli contesti per assicurare la conformità del sistema locale ai principi del regolamento

Sezioni di **carattere informativo**

contenenti riferimenti metodologici e suggerimenti di aiuto alla comprensione del testo ed all'implementazione di quanto previsto dal regolamento, ma **non contenenti regole** da applicare in ottemperanza al codice di condotta

Nota:
Comprendono anche best-practice, studi e lavori condotti autonomamente dai singoli partecipanti al di fuori dell'iniziativa di collaborazione, che –una volta ritenuti di comune interesse e di rilevanza- vengono inclusi e/o referenziati nel documento, evidenziando l'origine e la paternità intellettuale.

Ambiti del codice di condotta

Il codice di condotta deve definire delle regole secondo cui declinare –nello specifico dominio di attività- **tutti i principi e gli obblighi generali sanciti dal GDPR** (art. 40)

Gli obblighi prescritti dal regolamento possono essere classificati in **due categorie**

Obblighi relativi alle **operatività** nell'ambito delle attività giornaliere

- Informativa a e consenso de l'interessato
- Modalità di utilizzo e di accesso ai dati (procedure, abilitazioni, registri, documentazione)
- Rapporti con l'interessato (rettifica, cancellazione, consegna dati)
- Trasferimento dei dati a terzi
- Sicurezza
- Monitoraggio
- Gestione delle violazioni
- .....

Obblighi relativi alla **struttura organizzativa del titolare**

- Valutazione dell'impatto, preventivamente a nuove iniziative
- Metodologie di progettazione («privacy by design»)
- Riesami periodici e valutazione del sistema (organizzativo + tecnico) nel suo complesso
- Ruolo e responsabilità del DPO
- Criteri per la gestione delle controversie
- .....

Piano di lavoro incrementale

La composizione del gruppo di lavoro e la metodologia sono progettati in modo da consentire la definizione un codice di condotta complessivo

- valido per una qualsiasi tipologia di organizzazione sanitaria
- relativamente a tutti gli obblighi stabiliti dal Regolamento

Il piano di lavoro sarà strutturato secondo un **approccio modulare ed incrementale**:

- affrontando le singole tematiche secondo criteri di priorità
- in modo da ottenere risultati singolarmente utilizzabili in tempi più brevi
- garantendo comunque la coerenza finale del codice in tutte le sue parti

Per facilitare la collaborazione, la raccolta di contributi e la diffusione dei documenti

info@gdpr-sanita.it