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

UNIVERSITÀ CATTOLICA del Sacro Cuore

ALTEMS

ALTA SCUOLA DI ECONOMIA
E MANAGEMENT DEI SISTEMI SANITARI

Laboratorio sui sistemi informativi sanitari per il governo dell'organizzazione

In una organizzazione sanitaria moderna, il sistema informativo deve costituire uno strumento di governo per l'intera struttura, di rilevanza strategica ed in grado di influire significativamente sulla qualità, sicurezza ed economicità sia dei processi organizzativi che dei servizi sanitari erogati e –in definitiva- sulla stessa salute del paziente

Le attività del Laboratorio sono focalizzate sulle strategie, le metodologie e le best-practices per la valutazione, l'implementazione e l'evoluzione del sistema informativo sanitario in relazione alle esigenze organizzative ed al percorso assistenziale del paziente.

Il regolamento europeo per la protezione dei dati personali

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

La protezione delle persone fisiche con riguardo al trattamento dei dati personali ***è un diritto fondamentale***. (premesse, punto 1)

La protezione ***non dovrebbe dipendere dalle tecnologie impiegate*** *....* (premesse, punto 15)

La tutela dei diritti e delle libertà delle persone richiede l'adozione di ***misure tecniche e organizzative adeguate*** *....* (premesse, punto 78)

NON E' UNA CHECKLIST

- **Il regolamento definisce un insieme di principi e di obblighi di validità generale**, validi per tutti i settori di attività, per il trattamento dei dati personali secondo criteri di liceità, sicurezza e trasparenza nei confronti dell'interessato.

- Nel rispetto di questi principi di validità generale, **ogni organizzazione deve definire un proprio insieme di regole ed implementare un proprio sistema - basato su misure sia organizzative che tecniche** (art 1)- secondo il quale trattare le informazioni personali gestite.

- **Il sistema** -composto da regole di comportamento, procedure organizzative, documenti di riferimento e strumenti tecnologici- **deve essere costantemente verificato e manutenuto** (art. 24) e, preferibilmente, certificato periodicamente da un ente terzo appositamente accreditato (art. 42).

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

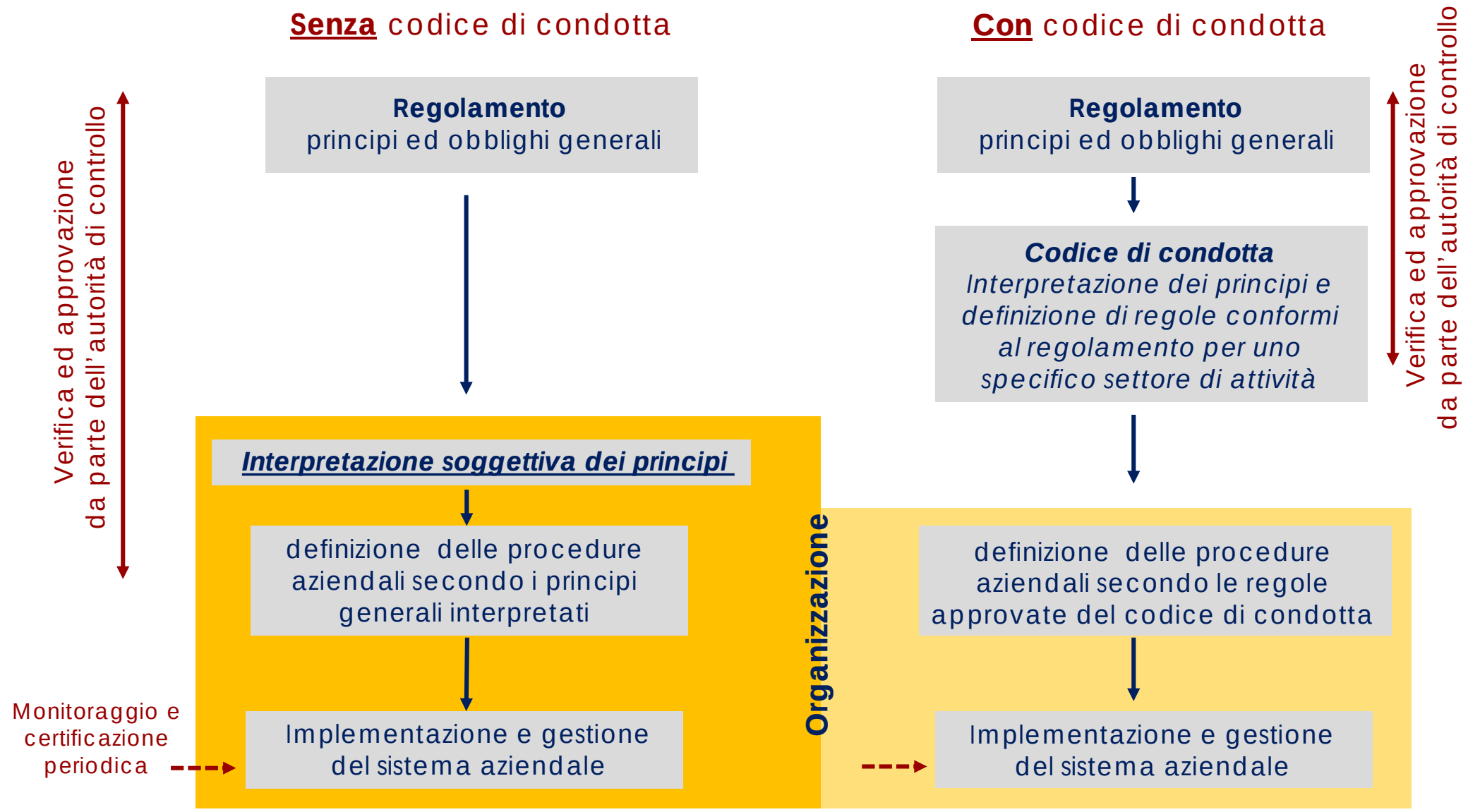
Per facilitare le organizzazioni nell'individuazione delle modalità secondo cui declinare i principi generali nel proprio settore di attività, è prevista la definizione dei cosiddetti "Codici di condotta" (art. 40).

- 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.

- **I codici di condotta sono definiti da associazioni e da altri organismi rappresentativi delle categorie interessate, vengono sottoposti all'approvazione dell'autorità di controllo**. In caso di parere favorevole, il codice di condotta viene registrato e pubblicato.

- **L'adesione di una organizzazione ad un codice di condotta può essere utilizzata per dimostrare il rispetto degli obblighi** da parte da parte della organizzazione stessa (art. 24).

Onere dell'organizzazione



Ambiti del codice di condotta

Il codice di condotta deve definire delle regole secondo cui specializzare –nello specifico dominio di attività- i principi e gli obblighi generali sanciti dal Regolamento **di natura organizzativa e tecnologica**

• Finalità e modalità del trattamento	artt. 5,6
• Rapporti con l'interessato	
- Acquisizione del consenso	artt. 7,8
- Informazioni e consenso al momento della raccolta dei dati	artt. 12-14
- Informazioni ed interazioni durante il periodo del trattamento (es. rettifiche, accessi, revoche, ..)	artt. 15-20
• Metodologie di progettazione ed implementazione	
- Valutazione preventiva dell'impatto	artt. 35-36
- «Impostazione predefinita della protezione» nei progetti	art. 25
- sicurezza	art. 32
• Documentazione (registri)	
- descrizione dei processi, dei dati, delle procedure e degli utilizzatori	art. 30
• Gestione delle violazioni, notifiche all'autorità di controllo e all'interessato	artt. 33-34
• Trasferimento dei dati	
- consegna all'interessato	art. 20
- trasferimento a terzi	artt. 44-48
• Gestione delle controversie	art. 79
• Monitoraggio, valutazione e riesami periodici del sistema nel suo complesso	art. 24

Approccio

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

Approccio e aspetti qualificanti

- **Aderenza delle regole alle reali esigenze** e specificità del contesto sanitario
- **Uso di un modello di riferimento 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

Metodo di lavoro

GDPR
Principi generali validi per tutti

Contesto sanitario

Aspetti normativi
- Legislazione
- Linee di indirizzo

Modello di riferimento
Indipendente dalla struttura organizzativa e tecnologica
- Processi e trattamenti
- Esigenze e scenari operativi
- Organizzazione

Ambito dell' iniziativa

Codice di condotta
Regole di riferimento per il settore sanitario

Singola organizzazione

Descrizione del proprio contesto e correlazione con il modello (metodologia e form)

Sistema, procedure e soluzioni specifiche della azienda

Rappresentatività dell'iniziativa

Istituzioni ed associazioni sanitarie e professionali di rilevanza nazionale.

Aziende sanitarie, anche per la verifica della applicabilità di quanto previsto nei contesti reali.

Associazione di cittadini, intesi sia come proprietari dei dati, sia come interlocutori attivi e continui nel processo sanitario.