

# INDICE SOMMARIO

<i>Introduzione</i> .....	XIII
---------------------------	------

## **CAPITOLO 1 L'IMPATTO DEL REGOLAMENTO UE 2016/679 SULLA SANITÀ: EFFICACIA DIFFERITA PROGRESSIVA**

1. Premessa .....	1
2. Cosa prevedeva la Direttiva comunitaria e come è stata attuata in Italia .....	2
3. Efficacia progressiva differita del Regolamento UE 2016/679: il periodo transitorio .....	3
4. Come cambia lo scenario con il Regolamento UE 2016/679 sul versante del c.d. "dato sanitario" .....	3
5. Altri obblighi del titolare del trattamento dei dati personali in ambito sanitario .....	5
6. Principi per il trattamento ai fini di archiviazione nel pubblico interesse o di ricerca scientifica (anche medica) o a fini statistici .....	6
7. I presupposti di liceità del trattamento di particolari categorie di dati personali .....	10

## **CAPITOLO 2 IL DATO SANITARIO**

1. Premessa .....	13
2. Natura giuridica e trattamento: cenni .....	16

## **CAPITOLO 3 OBBLIGHI E RESPONSABILITÀ PER LE IMPRESE NELLA SANITÀ**

1. Premessa .....	19
-------------------	----

2. Principi .....	20
3. Obblighi generali .....	22
4. Misure di sicurezza .....	22
5. Valutazione d'impatto sulla protezione dei dati e consultazione preventiva .....	27
6. Responsabilità .....	30

#### **CAPITOLO 4 NUOVE FIGURE SOGGETTIVE: IL DATA PROTECTION OFFICER**

1. Premessa .....	33
2. Nomina del D.P.O. nell'ambito sanitario .....	35
3. Concetto di svolgimento di una data attività "in via principale": casi di esclusione .....	36
4. Concetto di trattamento dei "dati su larga scala" .....	37
5. Concetto di "facile raggiungibilità" del D.P.O. ....	39
6. Possibile esternalizzazione delle funzioni di D.P.O. ....	39
7. Requisiti e qualità professionali del D.P.O. ....	40
8. Compiti del D.P.O. ....	41
9. Posizione ed autonomia del D.P.O. ....	42
10. Divieto di rimozione e/o penalizzazione del D.P.O. ....	43
11. Obblighi del titolare e del responsabile del trattamento nei confronti del D.P.O. ....	44
12. D.P.O.: profili d'incompatibilità della funzione .....	44
13. Durata della carica .....	45

#### **CAPITOLO 5 ACCOUNTABILITY (RESPONSABILIZZAZIONE)**

1. Premessa .....	47
2. Origine ed evoluzione del principio .....	49
3. <i>Accountability</i> e <i>privacy</i> .....	51

#### **CAPITOLO 6 PRIVACY BY DESIGN E PRIVACY BY DEFAULT**

1. Premessa .....	53
2. <i>Privacy by design</i> .....	56
2.1. Anonimizzazione .....	57
2.2. Psuedonimizzazione .....	59
3. <i>Privacy by default</i> .....	60

**CAPITOLO 7 GESTIONE E PIANIFICAZIONE DELLA PRIVACY**

1. Premessa .....	63
2. Analisi preventiva: <i>check list</i> .....	63
3. Designazione dei soggetti e registro delle attività di trattamento .....	66
4. Attività di controllo preventivo: analisi del rischio .....	67
5. Misure tecniche da adottare .....	68
6. Attività di <i>Auditing</i> .....	69
7. Sistemi di gestione dei reclami e di gestione delle richieste relative all'esercizio dei diritti degli interessati .....	70
8. Pianificazione della sicurezza .....	71
9. Consigli pratici .....	73

**CAPITOLO 8 DATA BREACH: LE CONSEGUENZE DELLE VIOLAZIONI AL TRATTAMENTO DEI DATI SULLA SALUTE**

1. Premessa .....	75
2. Distruzione, perdita, modifica, rivelazione non autorizzata ed accesso non autorizzato ai dati personali .....	76
3. Definizione del concetto di "violazione" .....	77
4. <i>Data breach</i> e l'errore umano in ambiente sanitario .....	77
5. Altro esempio di violazione dei dati: attacco alle applicazioni <i>Web</i> .....	78
6. <i>Cyber</i> spionaggio .....	79
7. <i>Insider Misuse</i> : particolare fattispecie di abuso di informazioni .....	79
8. Adeguatezza e tempestività dei rimedi approntati nel caso di <i>data breach</i> : notifica al Garante. Il caso "speciale" del <i>dossier</i> sanitario .....	80
9. Casi di esclusione degli obblighi di notifica al Garante .....	82
10. Comunicazione al Garante successiva alla violazione .....	82
11. Contenuto delle comunicazioni all'interessato a seguito di violazione sui dati personali .....	85
12. Casi di esclusione della comunicazione di avvenuta violazione all'interessato .....	86
13. Alcuni diritti inviolabili riconnessi al <i>data breach</i> : diritto all'integrità fisica e morale .....	87
14. Apparati mobili impiegabili nella sanità e la loro protezione .....	87

**CAPITOLO 9 FORMAZIONE**

1. Premessa .....	91
2. Principi e norme applicabili al trattamento di dati sensibili .....	92

3.	Trattamenti con strumenti elettronici e sistema di autenticazione informatica soggetti a formazione obbligatoria del personale .....	94
4.	Sistema di autorizzazione e altre misure di sicurezza soggette all'obbligo formativo .....	95
5.	Ulteriori misure in caso di trattamento di dati sensibili .....	95
6.	Trattamenti senza l'ausilio di strumenti elettronici e obbligo formativo .....	96
7.	Formazione richiesta dal Codice Privacy e dal Garante .....	96
8.	Regolamento UE e formazione .....	97

## **CAPITOLO 10 PRIVACY E ACCESSO CIVICO IN RELAZIONE ALLE STRUTTURE SANITARIE PUBBLICHE**

1.	Premessa .....	101
2.	Accesso civico .....	102
3.	Accesso civico e sanità .....	105
4.	Diritto di accesso e rapporto con la disciplina privacy .....	107
5.	Accesso ai documenti tenuti nelle strutture sanitarie .....	110

## **CAPITOLO 11 PROFILI DI RESPONSABILITÀ**

1.	Premessa .....	113
2.	Responsabilità civile: i soggetti responsabili .....	115
2.1.	Natura giuridica della responsabilità ex art. 15 Codice Privacy .	116
2.2.	L'onere della prova .....	117
2.3.	Danno non patrimoniale .....	120
2.4.	Elemento materiale: la violazione dell'art. 11 Codice Privacy ...	122
2.5.	Nozione di trattamento dei dati personali in caso di comunicazioni di dati attinenti alla salute .....	123
2.6.	Danni punitivi .....	125
2.7.	Autorità giudiziaria competente .....	127
2.8.	Tutela inibitoria .....	129
3.	Responsabilità penale .....	130
3.1.	L'art. 167 Codice Privacy: Trattamento illecito di dati .....	130
3.2.	La natura del reato .....	132
3.3.	L'autore del reato .....	133
3.4.	Il nocumento: problemi di qualificazione giuridica e di significato .....	134
3.5.	La comunicazione o diffusione illecita di dati personali .....	137

3.6. Comunicazione di dati personali ed esercizio del diritto di difesa .....	139
3.7. Il dolo specifico del profitto .....	139
4. Responsabilità amministrativa .....	140

## CAPITOLO 12 SISTEMA SANZIONATORIO

1. Premessa .....	141
2. Sanzioni nel Regolamento UE .....	141
3. Sanzioni nel Codice Privacy .....	144

## CAPITOLO 13 DIRITTO DELL'INTERESSATO - INFORMATIVA E CONSENSO

1. Premessa: diritti dell'interessato .....	151
2. Diritti personali e dati personali relativi alla salute .....	153
3. Diritto di accesso ai dati .....	154
3.1. Diritto di accesso ai dati nel Codice Privacy .....	154
3.2. Diritto di accesso ai dati nel Regolamento UE .....	156
4. Diritto di oscuramento dei dati .....	159
5. Come si esercita il diritto di accesso ai dati .....	159
6. Trattamento dei dati .....	160
7. Diritto dell'interessato al consenso e alla preventiva informativa .....	161
8. L'informativa all'interessato .....	161
8.1. L'informativa all'interessato nel Codice Privacy .....	161
8.2. L'informativa all'interessato nel Regolamento UE .....	165
9. Consenso dell'interessato .....	172
9.1. Consenso dell'interessato nel Codice Privacy .....	172
9.2. Consenso dell'interessato nel Regolamento UE .....	174

## CAPITOLO 14 FASCICOLO SANITARIO ELETTRONICO

1. Premessa .....	179
2. Definizione e caratteristiche .....	181
3. Soggetti minorenni .....	184
4. Finalità e ambiti di applicazione .....	184
5. Valore e sviluppo del Fse .....	185
6. Garanzie per l'interessato .....	186
6.1. Garanzie nel Codice Privacy .....	186
6.2. Garanzie nel Regolamento UE .....	187

6.3. Consenso informato al trattamento dei dati .....	188
6.4. Diritto all'oscuramento .....	190
7. Riscontro sui propri dati personali .....	191
8. Individuazione dei soggetti che possono trattare i dati .....	192
9. Accesso ai dati personali contenuti nel Fse .....	193
10. Misure di sicurezza .....	193

## CAPITOLO 15 **DOSSIER SANITARIO**

1. Premessa .....	195
2. Informativa al <i>dossier</i> sanitario .....	198
3. Consenso al <i>dossier</i> .....	200
3.1. Particolari casi di consenso .....	202
3.2. Prestazioni in emergenza .....	202
4. Sistemi informativi per l'organizzazione dei servizi territoriali di assistenza primaria .....	203
5. Diritti dell'interessato .....	204
5.1. Oscuramento .....	205
5.2. Diritto alla visione degli accessi al <i>dossier</i> .....	206
6. Accesso al <i>dossier</i> .....	207
7. Sicurezza dei dati nel <i>dossier</i> sanitario .....	207
7.1. <i>Data Breach</i> nel <i>dossier</i> sanitario .....	209

## CAPITOLO 16 **CARTELLA CLINICA ELETTRONICA**

1. Premessa .....	211
2. Cartella clinica digitale .....	213
3. Contenuti della Cartella Clinica Elettronica .....	214
4. Richiesta copia della Cartella Clinica Elettronica .....	216
5. Differenze tra la CCE, il Fse e il <i>dossier</i> sanitario .....	217
6. Protezione dei dati personali contenuti nella Cartella Clinica Elettronica .....	218
7. Conservazione della Cartella Clinica Elettronica .....	220

## CAPITOLO 17 **REFERTI ON-LINE**

1. Premessa .....	225
2. Definizione e caratteristiche .....	225
3. Fruizione facoltativa del servizio di refertazione <i>on-line</i> .....	226
4. Informativa e consenso .....	227

5. Archivio dei referti .....	227
6. Misure di sicurezza e tempi di conservazione dei dati .....	228

**CAPITOLO 18**    **PRIVACY NELLE STRUTTURE SANITARIE PRIVATE:  
PUBBLICAZIONE E DIFFUSIONE DI DATI PERSONALI  
NEI SITI *WEB* E *CUSTOMER SATISFACTION* IN  
AMBITO SANITARIO**

1. Premessa .....	231
2. Trattamento dei dati nei siti <i>web</i> dedicati esclusivamente alla salute .	233
2.1. Esercizio dei diritti dell'interessato .....	235
3. <i>Customer Satisfaction</i> in ambito sanitario .....	235
3.1. <i>Performance</i> nella Sanità .....	236
 <i>Bibliografia</i> .....	 239
<i>Indice analitico</i> .....	245

