

INDICE SOMMARIO

Prefazione di <i>Antonello Soro</i> - Presidente del Garante per la protezione dei dati personali	XIII
<i>Gli Autori</i>	XVII

CAPITOLO 1

LA NORMATIVA DI RIFERIMENTO

di *Michele Iaselli*

1. Il concetto di privacy	1
2. La normativa nazionale ed europea	3
3. Il Regolamento Europeo e l'adeguamento nazionale	9

CAPITOLO 2

IL SISTEMA DI GESTIONE DELLA PRIVACY

di *Andrea d'Agostino*

1. Introduzione e contesto normativo	29
2. La gestione dei dati personali: da una normativa prescrittiva alla responsabilizzazione delle imprese	31
3. L'evoluzione del sistema di gestione della privacy	35
4. Conclusioni	39

CAPITOLO 3

I SOGGETTI PRIVACY

di *Gianluigi Marino*

1. I soggetti previsti dal GDPR	41
2. Il Titolare del trattamento	42
3. I Contitolari	47
4. Il Responsabile del trattamento (e i sub-responsabili)	48
5. Rappresentanti di titolare e responsabile non stabiliti nell'Unione	54
6. <i>Data Protection Officer</i> (rinvio)	56
7. Interessato	57

CAPITOLO 4

I DIRITTI DEGLI INTERESSATIdi *Gianluigi Marino*

1.	Premessa	59
2.	Tempi, modalità e costi dell'esercizio dei diritti da parte dell'interessato	60
3.	Le limitazioni dei diritti previste dal GDPR e dal diritto italiano I diritti riguardanti le persone decedute	62
4.	Il diritto ad essere informati	64
5.	Il diritto di accesso dell'interessato	71
6.	Il diritto di rettifica	74
7.	Il diritto alla cancellazione	75
8.	Il diritto di limitazione del trattamento	80
9.	Il diritto alla portabilità dei dati	81
10.	Il diritto di opposizione	86
11.	Il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione	88
12.	Sanzioni	90

CAPITOLO 5

IL CONSENSO COME CONDIZIONE DI LICITÀdi *Lucio Scudiero*

1.	Il consenso dell'interessato nel più generale tema della liceità del trattamento	91
2.	I requisiti del consenso nel GDPR	92
3.	Analisi comparata GDPR - Ordinamento Italiano: il consenso libero	95
4.	(<i>Segue</i>): il consenso specifico	98
5.	(<i>Segue</i>): il consenso informato	101
6.	(<i>Segue</i>): il consenso inequivocabile	104
7.	(<i>Segue</i>): il consenso esplicito	105
8.	(<i>Segue</i>): il consenso dimostrabile	106
9.	(<i>Segue</i>): il consenso revocabile	108
10.	Il consenso dei minori	114
11.	Conclusioni	117

CAPITOLO 6

IL REGISTRO DEI TRATTAMENTIdi *Roberta Quintavalle*

1.	La normativa di riferimento	119
2.	Cosa deve fare il titolare	120
3.	Cosa deve fare il responsabile	121
4.	Chi ha l'obbligo di tenuta del registro delle attività di trattamento	122
5.	L'impatto in azienda e le funzioni coinvolte	124
6.	Come predisporre il Registro	124
7.	La <i>check list</i> per il Registro	126
8.	Come gestire il Registro	128

CAPITOLO 7

LA PROFILAZIONEdi *Iacopo Destri e Anna Maria Lotto*

1.	Introduzione	131
2.	Definizione e quadro normativo	132
3.	Disciplina sulla profilazione	134
3.1.	Previsioni generali applicabili in materia di profilazione e di processi decisionali automatizzati	135
3.2.	Processi decisionali esclusivamente automatizzati, compresa la profilazione	141
3.3.	Valutazione di impatto e responsabile della protezione dei dati	144
3.4.	Profilazione e minori	145
3.5.	Profilazione avente ad oggetto dati raccolti <i>on-line</i> e disciplina di dettaglio applicabile	146
4.	Riflessioni conclusive	149

CAPITOLO 8

SICUREZZA DEI DATI E VALUTAZIONE DEI RISCHIdi *Ulrico Bardari*

1.	Introduzione: dalla Privacy alla Sicurezza	155
2.	Sicurezza dei dati	156
2.1.	Valore delle informazioni e dei dati	156
2.2.	Sicurezza e minacce dei dati	157
2.3.	Misure di sicurezza	159
2.4.	La protezione dalla progettazione	160
2.5.	Messa in sicurezza e salvataggio dei dati	161
2.6.	Cancellazione e distruzione sicura	162
3.	Valutazione dei rischi	164
3.1.	Violazioni dei dati e valutazione d'impatto	164
3.2.	Analisi dei rischi	165
3.3.	I principi	166
3.4.	I rischi nel <i>cloud</i>	167
3.5.	Politiche aziendali per la gestione di rischi e minacce	168
3.6.	Gestione dell'innovazione	171
4.	Conclusioni	172

CAPITOLO 9

IL DATA PROTECTION OFFICERdi *Giovanni Battista Gallus e Michela Pintus*

1.	Introduzione	175
2.	Il DPO nel GDPR	177
2.1.	L'obbligatorietà della nomina: enti e organismi pubblici	177
2.2.	L'obbligatorietà della nomina: enti privati	180
2.3.	La nomina facoltativa	183
2.4.	La nomina del DPO	184
2.5.	La nomina del DPO nel settore pubblico	185
2.6.	La nomina del DPO nel settore privato	188

2.7.	La competenza specialistica e la capacità di assolvere i compiti come cardine nell'individuazione del DPO	189
2.8.	La posizione del DPO nelle organizzazioni pubbliche e private	191
2.9.	La pubblicità dei dati di contatto del DPO e le sue interazioni con gli interessati	192
2.10.	Compiti e responsabilità del DPO	193

CAPITOLO 10

DATA PROTECTION IMPACT ASSESSMENTdi *Giovanni Battista Gallus e Michela Pintus*

1.	Introduzione	199
2.	Definizione e presupposti	201
3.	Le ipotesi specifiche individuate dal GDPR	203
4.	Il procedimento di valutazione di impatto e la sua documentazione	205
5.	La consultazione preventiva	209
6.	La disciplina transitoria	210

CAPITOLO 11

LA NOTIFICAZIONE E LA COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI (“DATA BREACH”)di *Giovanni Battista Gallus*

1.	Introduzione	213
2.	La definizione di “violazione dei dati personali”	216
3.	La notificazione al Garante	218
3.1.	Il termine per la notificazione	219
3.2.	Il ruolo del <i>data processor</i>	220
3.3.	Modalità della notificazione	222
4.	La comunicazione agli interessati	224
4.1.	Il contenuto e le modalità della comunicazione agli interessati	225
4.2.	Le ipotesi di esclusione dell'obbligo di comunicazione agli interessati	227
5.	La formalizzazione e documentazione delle attività inerenti i <i>data breach</i>	229
6.	Il ruolo del DPO nella gestione dei <i>data breach</i>	231
7.	I rapporti con altre tipologie di <i>data breach</i>	231

CAPITOLO 12

IL TRASFERIMENTO DI DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALIdi *Vincenzo Colarocco*

1.	La normativa di riferimento	235
2.	Il Garante per la protezione dei dati personali, il Gruppo di lavoro <i>ex</i> Articolo 29	237
3.	Trasferimento di dati all'estero: l'esperienza del Codice Privacy	239
4.	Regolamento e trasferimento dei dati all'estero	241
5.	La decisione di adeguatezza	243

5.1.	Elenco Paesi autorizzati	244
5.2.	Trasferimento dati in USA: dal <i>Safe Harbor</i> al <i>Privacy Shield</i>	245
6.	Trasferimento soggetto a garanzie adeguate	247
6.1.	Norme vincolanti d'impresa	248
6.2.	Clausole Contrattuali Standardizzate	253
7.	Trasferimenti vietati	255
8.	Deroghe	255
9.	In conclusione, cosa cambia in sintesi	257

CAPITOLO 13

**BIG DATA E INTERNET OF THINGS:
DATA PROTECTION E DATA GOVERNANCE
ALLA LUCE DEL REGOLAMENTO EUROPEO**

di *Fernanda Faini*

1.	<i>Big data e Internet of Things</i>	259
2.	Il diritto incontra i "grandi dati": profili giuridici e implicazioni sociali	263
3.	La <i>data protection</i> nei <i>big data</i> e nell' <i>Internet of Things</i>	267
3.1.	Principi e strumenti del regolamento (UE) 2016/679 da impiegare e valorizzare nell'era degli algoritmi	269
3.2.	Aspetti problematici	272
4.	Possibili soluzioni e gestioni future	275

CAPITOLO 14

INTELLIGENZA ARTIFICIALE E ROBOTICA

di *Michele Iaselli*

1.	Cos'è la robotica	281
2.	Le applicazioni della robotica	283
3.	Il problema della regolamentazione giuridica	287
3.1.	Etica e responsabilità	289
3.2.	Privacy e sicurezza	293
4.	L'intelligenza artificiale	295
5.	I droni	310
6.	Conclusioni	317

CAPITOLO 15

**TRATTAMENTO DI DATI PERSONALI
PER SCOPI DI RICERCA SCIENTIFICA**

di *Stefania Stefanelli*

1.	Dati identificativi diretti ed indiretti	319
2.	Condizioni di liceità del trattamento a fini di ricerca scientifica	322
3.	Principio di limitazione delle finalità	325
4.	Espressione del consenso alla sperimentazione ed al trattamento dei dati	327
5.	Diritto all'autodeterminazione e partecipazione di minori e incapaci alla ricerca	329

6.	Trattamento dei dati personali in assenza di consenso	332
7.	Durata del trattamento e trattamento ulteriore	337
8.	Comunicazione e diritti degli interessati: efficacia generale delle regole deontologiche	340

CAPITOLO 16

LA CERTIFICAZIONE DEI CONSENSI RACCOLTI ONLINEdi *Tommaso Grotto e Emanuele Casadio*

1.	I dati come <i>asset</i> strategico alla luce dei <i>big data</i> e del GDPR	343
2.	Il ciclo di vita dei consensi	344
3.	La verificabilità dei consensi	344
4.	Il regime sanzionatorio	345
5.	Il ciclo di vita dei dati personali analogici e digitali	345
6.	Il valore probatorio delle firme elettroniche semplici, avanzate e qualificate	347
7.	L'acquisizione di un dato informatico secondo lo standard ISO/IEC 27037:2012	350
8.	L'acquisizione forense e la gestione dei consensi	353
9.	Il valore probatorio dei consensi acquisiti secondo lo standard ISO/IEC 27037:2012 e i precedenti giurisprudenziali a supporto	356
10.	I vantaggi collegati alla certificazione dei consensi	357

CAPITOLO 17

LA RESPONSABILITÀ CIVILE E DANNO DA TRATTAMENTO ILLECITO DEI DATI ALLA LUCE DEL REGOLAMENTO UE 2016/679di *Michela Barbarossa, Chiara Benvenuto e Valeria Cerocchi*

1.	Il diritto al risarcimento del danno da trattamento illecito di dati personali: evoluzione	359
2.	L'art. 82 del GDPR: le scelte del legislatore europeo	360
2.1.	Il danno risarcibile	364
2.2.	I soggetti responsabili: la responsabilità solidale	365
2.3.	La prova liberatoria alla luce del principio di <i>accountability</i>	370
2.4.	Il decreto legislativo attuativo	372
3.	La tutela giurisdizionale ed il ruolo dell'autorità di controllo: la questione della competenza territoriale	373
4.	L'orientamento francese	375
5.	L'ipotesi di trattamento illecito alla luce delle novità introdotte dal Regolamento	375
6.	Conclusioni	381

CAPITOLO 18

SANZIONI E RESPONSABILITÀ AMMINISTRATIVE E PENALIdi *Francesco Paolo Micozzi*

1.	Introduzione	383
2.	Le misure di cui all'art. 58 rilevanti in ambito sanzionatorio	386

3.	Le sanzioni amministrative	389
4.	Le ipotesi di sanzioni amministrative pecuniarie previste dal GDPR	390
4.1.	Le sanzioni amministrative pecuniarie del quarto comma dell'art. 83 del GDPR	392
4.2.	Le sanzioni amministrative pecuniarie del quinto comma dell'art. 83 del GDPR	397
5.	Elementi per la individuazione e quantificazione della sanzione amministrativa pecuniaria	397
6.	Criteri applicativi e procedimento sanzionatorio e correttivo secondo il decreto legislativo di armonizzazione	402
7.	Le altre sanzioni amministrative o penali	411
8.	Il trattamento illecito di dati (art. 167)	413
9.	Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (art. 167- <i>bis</i>).	416
10.	Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art. 167- <i>ter</i>)	418
11.	Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art. 168)	419
12.	Inosservanza di provvedimenti del Garante (art. 170)	420
13.	Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (art. 171)	420
14.	Questioni ulteriori	421
15.	Le norme penali incriminatrici del d.lgs. 51/2018.	422
16.	<i>Ne bis in idem</i>	424
17.	Disposizioni transitorie e finali	425

APPENDICE

IL PROCESSO DI ADEGUAMENTO AL GDPR

D.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) aggiornato al d.lgs. 10 agosto 2018, n. 101	431
--	-----

