

INDICE

Introduzione. <i>Dialogo tra Luca Bolognini e Rosario Imperiali d'Afflitto</i>	XVII
<i>Gli Autori</i>	XXI

Capitolo 1

LA GESTIONE DELLA CONFORMITÀ AL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI E AL CODICE PRIVACY

Alberto Bettiol

1. Inquadramento generale	2
2. Perché la conformità alla normativa in materia di protezione dei dati personali richiede un piano	6
2.1. Il principio di responsabilizzazione quale fondamento del piano di conformità	6
2.2. La valutazione dei rischi e il principio di protezione dei dati fin dalla progettazione e per impostazione predefinita	7
2.3. La compilazione del registro delle attività di trattamento e le altre responsabilità di tenuta documentale	7
2.4. La gestione delle violazioni dei dati personali e le misure di sicurezza	7
2.5. Il ruolo del RPD e il modello organizzativo di gestione della protezione dei dati personali	8
2.6. La sensibilizzazione e formazione del personale e la creazione di una cultura interna in materia di protezione dei dati personali	8
2.7. Lo svolgimento della VIP	8
2.8. Le relazioni con le terze parti e la gestione dei rapporti contrattuali	9
2.9. I processi di verifica e miglioramento continuo della conformità	9
3. Come realizzare un piano di conformità alla normativa in materia di protezione dei dati personali	10
3.1. Introduzione e contesto normativo: dal Codice privacy al RGPD	10
3.2. I principi fondamentali del RGPD	10
3.3. Il sistema di governo della protezione dei dati personali: compiti, ruoli e responsabilità	10
3.4. La valutazione del rischio e il principio di responsabilizzazione	11
3.5. La mappatura dei trattamenti di dati personali	11
3.6. La compilazione del registro delle attività di trattamento	11
3.7. Le informative sul trattamento dei dati personali e la mappatura dei consensi al trattamento	12
3.8. La gestione delle richieste di esercizio dei diritti da parte degli interessati	12
3.9. Misure di sicurezza e gestione delle violazioni dei dati personali	12
3.10. La VIP	13
3.11. Formazione e consapevolezza del personale coinvolto nel trattamento dei dati personali	13

3.12. <i>Audit</i> , monitoraggio e riesame	13
3.13. I rischi sanzionatori e le responsabilità giuridiche in capo ai componenti dell'organizzazione	13
4. Come gestire un sistema per la protezione dei dati personali a livello di gruppo imprenditoriale	14
4.1. Il quadro normativo europeo e nazionale	14
4.2. Definizione e caratteristiche del gruppo imprenditoriale	16
4.3. Il principio di responsabilizzazione e la designazione dei soggetti del modello di gestione dei dati personali	18
4.4. Il ruolo del RPD a livello di gruppo imprenditoriale	19
4.5. Formazione e sensibilizzazione	21
4.6. Il sistema di gestione documentale	21
4.7. Il ruolo dell'autorità di controllo e la sua interazione con il gruppo imprenditoriale	22
4.8. Spunti operativi	22
5. Come condurre una <i>data protection due diligence & gap analysis</i>	23
5.1. Il concetto di <i>data protection due diligence & gap analysis</i> e i suoi ambiti applicativi	24
5.2. Fasi metodologiche di svolgimento della <i>data protection due diligence & gap analysis</i>	25
5.3. Identificazione e valutazione degli scostamenti	26
5.4. Valutazione del rischio e piano di miglioramento e rimedio	27
5.5. Ruoli e responsabilità	29
5.6. La <i>data protection due diligence & gap analysis</i> in contesti specifici	30
5.7. Migliori prassi ed efficacia dei modelli di <i>audit</i>	31
6. Come determinare indici di conformità in materia di protezione dei dati personali	33
6.1. Il concetto di indice di conformità	33
6.2. Finalità e vantaggi degli indici di conformità	33
6.3. I criteri per la definizione degli indici	34
6.4. Ambiti di applicazione degli indici di conformità	34
6.5. Strumenti per la rilevazione e l'elaborazione degli indici	35
6.6. Il ruolo dell'alta direzione e del RPD	36
6.7. Indici di conformità e principio di responsabilizzazione	36
7. Opportunità di gestione integrata della conformità: coordinamento con la disciplina in materia d'intelligenza artificiale	37
7.1. Il regolamento sull'IA	37
7.2. La legge italiana per l'IA	38
7.3. La gestione integrata della conformità alla normativa in materia di protezione dei dati personali e alla disciplina in materia d'IA	40
8. Considerazioni conclusive e schemi di sintesi	42
<i>Casi pratici</i>	44

Capitolo 2

CAMPO DI APPLICAZIONE

Marzia Piscopo

1. Inquadramento	47
2. Come verificare l'applicazione materiale e territoriale del GDPR	48
2.1. Come verificare l'applicazione materiale del GDPR	48
2.1.1. La sentenza della Corte di Giustizia dell'Unione Europea e la relativizzazione del concetto di dato personale	57
2.2. Come verificare l'applicazione territoriale del GDPR	59
3. Come conformarsi alle leggi applicabili UE ed extra-UE in un gruppo multinazionale	66

3.1. La Governance aziendale e le diverse competenze per materia	66
3.2. Come conformarsi alle leggi privacy UE ed extra UE in un gruppo multinazionale	68
4. Come gestire le normative privacy nazionali applicabili per settori o materia in UE	71
4.1. Normative privacy nazionali per settori o materia in UE: impatti pratici	72
5. Come coordinare l'applicazione del GDPR con altre norme della strategia UE sui dati	78
5.1. La strategia UE sui dati e le nuove regolamentazioni	78
5.2. Come coordinare i nuovi regolamenti con l'applicazione del GDPR	80
<i>Casi pratici</i>	82

Capitolo 3

PRINCIPI E BASI GIURIDICHE

Sergio Aracu

1. Inquadramento	85
2. Come accertare la liceità del trattamento	86
3. Come verificare il rispetto dei principi	89
4. Come identificare la base giuridica e le altre condizioni di liceità del trattamento	92
4.1. <i>Checklist</i> operative sui requisiti delle singole basi giuridiche	93
4.2. Come eseguire correttamente un test di bilanciamento per il legittimo interesse	103
5. Come gestire il consenso dell'interessato, la sua validità e la documentabilità a fini di prova	106
5.1. <i>Checklist</i> operativa utile a verificare la validità del consenso	106
5.2. <i>Checklist</i> operativa utile a verificare la documentabilità del consenso a fini di prova (<i>accountability</i>)	109
5.3. Per quanto conservare prova dei consensi acquisiti?	111
5.4. Il consenso acquisito da terzi. Casistiche e oneri di verifica in capo al Titolare del trattamento	114
6. Come gestire le deroghe al divieto generale di trattamento per le categorie particolari di dati personali <i>ex art. 9</i> GDPR	115
7. Come verificare la liceità del trattamento di dati relativi a condanne penali e reati <i>ex art. 10</i> GDPR	122
<i>Casi pratici</i>	124

Capitolo 4

TRASPARENZA E CORRETTEZZA

Chiara Ciccia Romito

1. Introduzione di sistema: il principio di correttezza alla base del processo di compliance al Reg. (UE) 2016/679	127
2. Il principio di correttezza in pratica	129
3. Il principio di trasparenza e la sua applicazione	131
3.1. Le informazioni da fornire all'interessato	135
3.2. Le informative privacy	138
4. Il <i>Legal design</i>	140
4.1. Il <i>Legal design</i> applicato alle informazioni da rendere all'interessato	141
4.2. Breve analisi giurisprudenziale	143
5. Le <i>policy web</i> , le modalità di somministrazione e l'aggiornamento dei contenuti	144
5.1. La <i>cookie policy</i>	144
5.2. <i>Cookie wall</i>	145
5.3. Il <i>banner cookie</i>	146

5.4. I termini e le condizioni generali di utilizzo di un sito web	147
5.5. <i>Chatbot</i> e <i>Legal design</i>	148
6. Come gestire la mappatura e la conformità dei tracciatori online	149
6.1. La gestione dei marcatori, tra GDPR e <i>cybersecurity</i>	150
6.2. La mappatura dei tracciatori online	151
7. Il diritto di accesso	151
7.1. Diritto di accesso e trasparenza nelle Pubbliche Amministrazioni	154
7.2. Decreto trasparenza e accesso	156
7.3. La gestione del diritto di accesso: una <i>checklist</i> operativa di conformità	158
8. Gli obblighi di trasparenza nell'AI Act	159
9. Gli obblighi di trasparenza nella legge italiana sull'intelligenza artificiale.	162

Capitolo 5

MINIMIZZAZIONE E LIMITAZIONE DELLA CONSERVAZIONE

Samanta Stanco

1. Inquadramento	165
2. Origini e sviluppi normativi	167
3. Applicazione del principio di minimizzazione dei dati	169
4. Portata operativa del principio	169
4.1. Riepilogo operativo: tabella di applicazione del principio di minimizzazione	171
5. Strategie per Big Data e intelligenza artificiale	172
5.1. Rischi specifici dei modelli generativi	173
5.2. Esempi pratici di applicazione del principio	175
6. Limitazione dell'accesso ai dati	177
6.1. Misure pratiche per il controllo degli accessi	178
6.2. Gestione contestuale e verifica degli accessi	179
7. Identificazione dei termini di conservazione e redazione della <i>data retention policy</i>	180
7.1. Come determinare i termini di conservazione	180
7.2. Stesura della <i>data retention policy</i>	181
8. Applicazione della <i>data retention policy</i> nei sistemi informatici	182
8.1. Automazione della conservazione e cancellazione	183
8.2. Funzionalità chiave da implementare nei sistemi IT	183
8.3. Ruoli e responsabilità	185
9. La disposizione dei dati alla scadenza dei termini di conservazione	186
9.1. Metodi di eliminazione sicura dei dati	186
9.2. Processo operativo consigliato	187
9.3. Esempi pratici	187
10. Minimizzazione per impostazione predefinita e responsabilizzazione	189
10.1. Elementi da considerare per la progettazione conforme	189
10.2. Esempi di configurazione per impostazione predefinita	190
11. Esempi settoriali e applicazioni pratiche	190
11.1. Il settore sanitario	191
11.2. Il settore dell' <i>e-commerce</i>	191
11.3. La Pubblica Amministrazione	192
12. Monitoraggio della conformità: indicatori e <i>audit</i>	192
12.1. <i>Audit</i> interni e verifiche di conformità	193
12.2. Cruscotti e reportistica integrata	194
13. Strumenti operativi e di supporto alla conformità	194
13.1. <i>Checklist</i> operative per i referenti privacy	194

13.2. Valutazione d'impatto sulla protezione dei dati (DPIA)	195
13.3. Strumenti tecnologici e piattaforme di gestione privacy	196
14. Conclusioni	196

Capitolo 6

FINALITÀ E COMPATIBILITÀ

Andrea Michinelli

1. Come specificare le finalità dei trattamenti, quale livello di granularità adottare	199
1.1. Inquadramento	199
1.2. Il principio di limitazione delle finalità e gli altri principi	202
1.3. Il principio di limitazione delle finalità e la sua scomposizione	205
1.3.1. Primo requisito: come formulare finalità "determinate" <i>ex ante</i>	208
1.3.1.1. Raggruppare o suddividere: la granularità delle finalità	211
1.3.1.2. Evitare di confondere finalità e modalità di trattamento	214
1.3.2. Secondo requisito: come formulare finalità "esplicite"	215
1.3.3. Terzo requisito: come identificare finalità "lecite"	216
1.4. Limitazione delle finalità secondo i principi <i>privacy by design</i> e <i>by default</i> <i>ex art. 25 GDPR</i> e un caso pratico	220
1.5. Suggerimenti operativi	224
2. Come svolgere la valutazione di compatibilità di finalità per trattamenti ulteriori	228
2.1. Inquadramento	228
2.1.1. La nozione di compatibilità e il <i>pre-screening</i>	230
2.1.2. La rilevanza delle basi giuridiche di partenza	231
2.1.3. Il test di compatibilità delle finalità	233
2.2. L'uso compatibile per fini di archiviazione nel pubblico interesse, di ricerca scientifica/storica o statistici <i>ex art. 89.1 GDPR</i>	240
2.3. Il caso dell'Intelligenza Artificiale: il training dell'AI come attività compatibile	243
2.4. Ulteriori casistiche di trattamento per finalità compatibili (e incompatibili)	247
2.5. Altri suggerimenti operativi	250

Capitolo 7

DATA PROTECTION BY-DESIGN E BY-DEFAULT, SICUREZZA DEI DATI E VIOLAZIONI DEI DATI (DATA BREACH)

Alessandra Toma

1. Inquadramento	253
2. <i>Data protection by design</i> e <i>by default</i>	255
2.1. Tecniche di protezione dei dati sin dalla progettazione	256
2.2. Tecniche e accorgimenti di protezione dei dati per impostazione predefinita	257
3. Valutazione del rischio di sicurezza dei dati e dei sistemi	259
4. Determinare l'adeguatezza delle misure tecnico-organizzative in un'organizzazione	264
4.1. <i>Security assessment</i> e <i>checklist</i>	265
4.2. Criteri di valutazione del livello di maturità	282
5. Standard internazionali di sicurezza dei dati	286
5.1. International Organization for Standardization	289
5.2. National Institute of Standards and Technology	295
5.3. European Union Agency for Network and Information Security	296

6. Come affrontare le violazioni: gestione della crisi e interventi a rimedio	298
7. Come valutare il rischio di sicurezza preventivo e quello derivante dalle violazioni	300
8. Come effettuare le notifiche all'Autorità e le comunicazioni agli interessati	304
<i>Casi pratici</i>	307

Capitolo 8

GOVERNANCE, LEADERSHIP E SUPERVISIONE

Lucrezia Giachetti

1. Come definire un adeguato modello organizzativo per la gestione dei dati personali	310
1.1. Cos'è un modello organizzativo?	310
1.2. Cos'è un modello organizzativo nella protezione dei dati?	310
1.2.1. Definizione, importanza e principi chiave di un modello organizzativo per la privacy	310
1.3. Creazione di un modello di <i>Data Governance</i> efficace	312
1.3.1. Fasi di progettazione del modello organizzativo	312
1.4. <i>Leadership</i> e <i>Data Governance</i>	325
2. Come realizzare un modello di gruppo per la protezione dei dati	326
2.1. La <i>governance</i> della privacy in contesti aziendali complessi	327
2.2. Coordinamento e centralizzazione vs. decentramento della gestione	328
2.3. Implementazione di un modello di gruppo per la protezione dei dati	328
2.3.1. Mappatura delle attività di trattamento	328
2.3.2. Informative e basi giuridiche del trattamento	329
2.3.3. Definizione di procedure standard e linee guida per tutte le entità del gruppo	330
2.3.4. La corretta individuazione dei ruoli privacy nel contesto di un gruppo	331
3. La creazione condivisa delle procedure nelle diverse funzioni	333
3.1. Importanza della creazione condivisa delle procedure per garantire l'efficacia del modello organizzativo privacy	334
3.2. Coinvolgimento delle diverse funzioni aziendali nella creazione delle procedure	334
3.3. Procedure per la raccolta, gestione, conservazione e distruzione dei dati personali	335
3.4. Gestione dei diritti degli interessati (accesso, rettifica, cancellazione ecc.)	336
3.5. Implementazione di procedure per la gestione dei <i>data breach</i>	336
3.6. Creazione di protocolli di <i>audit</i> e verifica per il monitoraggio continuo delle procedure	337
4. Il ruolo del Responsabile della protezione dei dati (Data Protection Officer): rapporti col vertice, budget, valutazioni e piano d'azione	337
4.1. Chi è il Data Protection Officer (DPO) e quali sono le sue competenze	338
4.2. I rapporti tra il DPO e il vertice aziendale	339
4.3. Definizione di un budget per il Responsabile della protezione dei dati	340
4.4. Le valutazioni del Data Protection Officer	340
4.5. Pianificazione e sviluppo di un piano d'azione per il miglioramento continuo	342
5. Conclusioni	343

Capitolo 9

L'APPROCCIO BASATO SUL RISCHIO

Alberto Nicolai

1. Inquadramento	345
2. La valutazione del rischio dei trattamenti	347

2.1. Il concetto di rischio e le tipologie di danni	347
2.2. Il rapporto con il Registro dei trattamenti	350
2.3. Il Trigger Test	353
2.4. Il calcolo del rischio inerente	356
2.5. Valutazione delle misure di sicurezza	359
2.6. Calcolo del rischio residuo	363
2.7. Documentazione e responsabilità	364
3. La valutazione d'impatto sulla protezione dei dati	365
3.1. Introduzione alla DPIA	365
3.2. Differenza tra DPIA e valutazione del rischio	366
3.3. Casistiche in cui la DPIA è obbligatoria	366
3.4. I contenuti minimi della DPIA	367
3.5. Come effettuare una DPIA	368
3.6. Coinvolgimento degli interessati	371
3.7. Coinvolgimento del DPO	373
3.8. Consultazione preventiva con l'Autorità di controllo	374
3.9. Aggiornamento e documentazione della DPIA	374
4. La valutazione del legittimo interesse	375
5. Il coordinamento tra DPIA e FRIA	376
5.1. Introduzione alla FRIA	376
5.2. Punti di contatto tra DPIA e FRIA	378
5.3. Differenze tra DPIA e FRIA	379
5.4. Conclusioni	380
<i>Casi pratici</i>	380

Capitolo 10

REGISTRO E MAPPATURA DEI PROCESSI, DEI TRATTAMENTI E DEI DATI - SISTEMA DOCUMENTALE E ACCOUNTABILITY

Giovanni Brunetti

1. Inquadramento	381
2. Una metodologia per la costruzione del registro dei trattamenti	382
3. Come svolgere, monitorare e aggiornare la mappatura dei trattamenti	383
3.1. Come identificare le tipologie di dati e come gestirli	388
4. Come creare e mantenere il registro	393
4.1. Come valutare quali trattamenti includere nel registro e il relativo livello di dettaglio	394
4.2. Come gestire i contenuti del registro	396
4.2.1. I contenuti del registro in qualità di Titolare	396
4.2.2. I contenuti del registro in qualità di Responsabile	401
4.3. Modalità di gestione del registro e soggetti coinvolti	403
4.4. Modalità di condivisione del registro	405
4.5. Ulteriori indicazioni pratiche per la creazione del registro	406
5. Come usare i <i>software</i> di gestione dei registri	407
6. Come realizzare e mantenere il sistema documentale sulla gestione interna dei dati personali	409
7. Come utilizzare i <i>software</i> gestionali per la <i>compliance</i> privacy	415
8. Come assicurare la coerenza tra registro, informative e riscontro al diritto di accesso	418
8.1. La coerenza tra il registro e ulteriori adempimenti del GDPR	419
<i>Casi pratici</i>	422

Capitolo 11
RUOLI E FILIERA DEL DATO
Pietro Calorio

1. Inquadramento	425
2. Note preliminari	427
2.1. Il tema linguistico	427
2.2. Disambiguazioni e precisazioni terminologiche	428
2.3. Il corretto approccio operativo all'individuazione dei « ruoli privacy »	431
2.4. Conseguenze degli errori nell'individuazione del ruolo	434
3. Ruoli funzionali delle organizzazioni (e fra organizzazioni)	435
3.1. Titolare del trattamento (<i>controller</i>)	435
3.1.1. Identikit	435
3.1.2. Adempimenti connessi al ruolo ed esempi	438
3.2. Contitolari del trattamento (<i>joint controllers</i>)	440
3.2.1. Identikit	440
3.2.2. Adempimenti connessi al ruolo ed esempi	442
3.3. Responsabile del trattamento (<i>processor</i>)	445
3.3.1. Identikit	445
3.3.2. Adempimenti connessi al ruolo ed esempi	447
4. Il modello organizzativo privacy e l' <i>awareness</i> interna	471
4.1. Il modello organizzativo privacy: cenni e rinvio	471
4.1.1. L'organigramma privacy come strumento organizzativo	471
4.1.2. Un modello stratificato per l'organigramma privacy	472
4.1.3. Etichette e nomenclatura nei diversi contesti organizzativi	473
4.2. Il fattore umano: <i>awareness</i> , formazione, addestramento	477
4.2.1. Pianificazione e stratificazione della formazione	477
4.2.2. Modalità di erogazione e approccio didattico	479
4.2.3. Strumenti, verifica e documentazione	480
5. Ruoli endo-organizzativi	482
5.1. Persone autorizzate al trattamento	484
5.1.1. Identikit	484
5.1.2. Adempimenti connessi al ruolo ed esempi	488
5.2. I soggetti designati	498
5.2.1. Identikit	498
5.2.2. Adempimenti connessi al ruolo ed esempi	499
5.3. L'Amministratore di Sistema	508
5.3.1. Identikit	508
5.3.2. Adempimenti connessi al ruolo ed esempi	509
6. Altri soggetti/ruoli	510
6.1. Interessato	510
6.1.1. Identikit	510
6.1.2. Adempimenti connessi al ruolo ed esempi	512
6.2. Destinatario	512
6.2.1. Identikit	512
6.2.2. Adempimenti connessi al ruolo ed esempi	513
6.3. Terzo	514
6.3.1. Identikit	514
6.3.2. Adempimenti connessi al ruolo ed esempi	514
6.4. DPO	517

6.4.1. Identikit	517
6.4.2. Adempimenti connessi al ruolo ed esempi	517
6.5. Rappresentante nell'Unione	518
6.5.1. Identikit	518
6.5.2. Adempimenti connessi al ruolo ed esempi	518
<i>Casi pratici</i>	528

Capitolo 12

FLUSSI ESTERI DI DATI

Gianluca Martinelli

1. Introduzione	543
2. I tratti essenziali del Capo V del GDPR e questioni applicative	544
2.1. La nozione di trasferimento internazionale	544
2.2. Le condizioni per il trasferimento internazionale di dati alla luce della sentenza "Schrems II"	546
2.3. La gestione dei trasferimenti internazionali: una <i>checklist</i> pratica offerta dall'EDPB	548
3. Mappatura e analisi dei flussi di dati verso paesi terzi	550
4. <i>Transfer Impact Assessment</i> (TIA): concetto e applicazione	554
4.1. Questionario di screening per la valutazione della necessità di effettuare un TIA	554
4.2. L'esecuzione del TIA	557
5. Guida all'applicazione delle SCC	563
5.1. Introduzione	563
5.2. Analisi della struttura e prassi operative	564
5.3. L'incorporazione delle SCC negli accordi sul trattamento <i>ex art. 28 GDPR</i> ("DPA")	570
6. <i>Binding Corporate Rules</i>	571
6.1. Introduzione e pre-requisiti delle BCR	571
6.2. Gli step operativi per l'adozione delle BCR	572
7. Le deroghe ai trasferimenti internazionali	577
7.1. Principi generali e step operativi	577
7.2. Analisi pratica delle deroghe <i>ex art. 49 GDPR</i>	578
7.3. Il trasferimento internazionale in base a sentenze di autorità giurisdizionali o amministrative in paesi terzi	585
7.3.1. Procedura operativa per la gestione delle richieste	586
<i>Casi pratici</i>	586

Capitolo 13

DIRITTI E LORO ESERCIZIO

Luigi Occhiuto

1. Il quadro giuridico dei diritti dell'interessato	589
2. Come gestire al meglio un'istanza dell'interessato all'interno dell'organizzazione aziendale	590
2.1. Un sistema organizzativo per la gestione delle richieste degli interessati	590
2.2. L'obbligo di agevolare l'esercizio dei diritti	592
2.3. Le fasi di gestione comuni a tutti i diritti	592
2.4. Tempistiche delle risposte	598
2.5. Adempimenti in caso di comunicazione a responsabili del trattamento, contitolari e terzi	599
3. Come gestire il diritto alla rettifica e aggiornamento dei dati	600

4. Come gestire il diritto di cancellazione dei dati	602
5. Come gestire il diritto alla limitazione dei dati	607
6. Come gestire i diritti di portabilità dei dati	610
7. Come gestire i diritti di opposizione al trattamento	615
8. Come gestire il diritto di non essere sottoposti a decisioni automatizzate	619
9. Accorgimenti per la progettazione dei CRM	625
10. Come gestire i diritti sui dati delle persone decedute	627

Capitolo 14

AUTOREGOLAMENTAZIONE

Stefano Petrussi

1. Inquadramento	629
2. I codici di condotta nel GDPR	629
2.1. L'ammissibilità di un progetto di codice e la procedura di approvazione del Garante	631
2.2. I benefici dell'adesione ai codici di condotta	634
2.3. Il monitoraggio dei codici di condotta	635
2.3.1. I requisiti di accreditamento dell'organismo di monitoraggio	635
2.3.2. I compiti dell'organismo di monitoraggio	638
3. Come aderire ad un codice di condotta	639
4. Come monitorare e attestare il rispetto di un codice di condotta	642
5. Le certificazioni	643
5.1. Gli organismi di certificazione	646
5.2. Lo sviluppo dei criteri di certificazione	649
5.3. Gli orientamenti dell'EDPB per la definizione dei criteri di certificazione	653
6. Come prepararsi alla certificazione GDPR e come monitorare e attestare il rispetto delle certificazioni	660
<i>Casi pratici</i>	660

Capitolo 15

RECLAMI, ISPEZIONI, RICORSI E IMPUGNAZIONI

Silvia Stefanelli, Maria Livia Rizzo e Noemi Conditi

1. Premesse: la fase patologica del trattamento dei dati	665
2. La tutela dell'interessato	667
2.1. Le forme alternative di tutela	667
2.2. La rappresentanza degli interessati	668
2.3. Come si attiva la tutela amministrativa: il reclamo e la segnalazione al Garante	671
2.3.1. Il reclamo al Garante	671
2.3.2. Contenuto del reclamo	672
2.3.3. Trasmissione del reclamo	674
2.3.4. Reclamo irregolare o incompleto	675
2.3.5. Termini e obblighi informativi del Garante	675
2.4. La segnalazione al Garante	675
2.4.1. Come viene trattata la segnalazione	677
2.5. Come si attiva la tutela giurisdizionale: il ricorso all'autorità giudiziaria	677
2.5.1. Chi può ricorrere in giudizio	678
2.5.2. Fasi processuali	678

2.5.3. Suggerimenti pratici per la presentazione di un ricorso	684
2.5.4. Nozione di “danno immateriale”	685
3. I poteri di indagine del Garante	685
3.1. Le attività ispettive	685
3.1.1. Il protocollo di intesa con la Guardia di Finanza	687
3.1.2. Il protocollo d’intesa con l’Agenzia per la Cybersicurezza Nazionale	688
3.1.3. La procedura interna aziendale per gestire le indagini del Garante	689
4. L’istruttoria preliminare del Garante	691
4.1. Archiviazione della istruttoria preliminare	692
5. L’apertura del procedimento per l’adozione dei provvedimenti correttivi e sanzionatori	693
5.1. Le deduzioni davanti al Garante	694
6. Il provvedimento di ordinanza ingiunzione del Garante	697
6.1. La giurisprudenza intervenuta sui principi della ordinanza ingiunzione	698
6.1.1. Assenza di automatismo nell’adozione di azioni correttive o l’irrogazione di sanzioni in caso di accertata violazione	698
6.1.2. Margine di discrezionalità delle Autorità di controllo	698
6.1.3. Assenza di un diritto soggettivo dell’interessato all’irrogazione della sanzione	699
6.1.4. Omissione di azioni correttive	699
6.1.5. Obiettivo delle sanzioni amministrative	699
6.2. Sui criteri da applicare per il calcolo della sanzione	699
6.3. I profili procedurali	701
6.3.1. Pagamento dell’importo sanzionato	701
6.3.2. Pubblicazione dei provvedimenti	701
7. Impugnazione del provvedimento del Garante davanti al giudice ordinario	702
7.1. Sui poteri del giudice adito	702
7.2. Sui motivi di impugnazione	703

