



L'estratto che stai visualizzando
è tratto da un volume pubblicato su
ShopWki - La libreria del professionista

[VAI ALLA SCHEDA PRODOTTO](#)

SOMMARIO

Profilo Autore	I
Prefazione	II
Presentazione	IV
Introduzione	VII

Parte I

Il General Data Protection Regulation (GDPR)

Capitolo 1 – Il sistema GDPR

1.1. Un lungo percorso	3
1.2. Le categorie dei dati personali.....	8
1.3. Il perimetro del sistema “protezione dei dati personali”	9
1.4. Il trattamento dei dati: principi e tipologie.....	13
1.5. Trasferimenti di dati personali verso paesi terzi od organizzazioni internazionali	18
1.6. Strumenti per la qualità del data protection.....	21
1.6.1. Il codice di condotta e l’organismo di controllo	21
1.6.2. La certificazione.....	23
1.6.3. L’accreditamento.....	24
1.7. Data breach: notifiche, comunicazioni e responsabilità. Il sistema sanzionatorio.....	25
1.8. Le autorità di controllo indipendenti.....	29
1.9. Dal Gruppo “articolo 29” al Comitato Europeo per la protezione dei dati	31

Capitolo 2 – I diritti tutelati

2.1. Diritto alla protezione dei dati personali (data protection), diritto alla riservatezza (privacy) e diritti derivati.....	35
2.2. Limitazioni all’esercizio dei diritti dell’interessato	37
2.3. Diritto all’informativa e diritto di accesso.....	38
2.4. Diritto di rettifica.....	40
2.5. Diritto alla cancellazione o diritto all’oblio.....	40
2.6. Diritto alla limitazione del trattamento	42
2.7. Diritto alla portabilità dei dati	43
2.8. Diritto di opposizione.....	43
2.9. Diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato	44
2.10 Reclami e ricorsi giurisdizionali.....	45

Capitolo 3 – Conoscere e decidere: l’informativa e il consenso

3.1. L’informativa.....	48
3.1.1. I contenuti.....	48
3.1.2. I tempi	49
3.1.3. La forma	50
3.1.4. I costi	51
3.2. Il consenso	51
3.3. Segue: l’esempio dei <i>cookies</i>	52

Parte II

La dimensione organizzativa

Capitolo 4 – I soggetti e i ruoli

4.1. La distribuzione delle competenze e delle responsabilità. Un’ipotesi di organigramma.....	57
4.2. Il Titolare del trattamento	59
4.3. Il Responsabile del trattamento	62
4.4. L’Incaricato del trattamento).....	64
4.5. Il Responsabile della protezione dei dati (Il Data Protection Officer) ...	65
4.5.1. Obbligatorietà e facoltatività della nomina del DPO.....	65
4.5.2. Compiti e requisiti professionali	66
4.5.3. Prerogative e doveri del DPO	69
4.6. I profili professionali previsti dalla norma UNI 11697:2017	70

Capitolo 5 – Il Data protection by design: progettare il trattamento dei dati

5.1. Il rischio da trattamento dei dati personali.....	74
5.2. Il Data protection by design.....	76
5.3. I presupposti organizzativi.....	79
5.3.1. Corporate governance e integrazione del data protection con gli altri controlli: la necessità di un approccio sistemico.....	79
5.3.2. La mappatura dei processi	82
5.3.3. I registri delle attività di trattamento	88
5.4. Il framework per la gestione del rischio	92
5.4.1. Il mandato.....	93
5.4.2. Progettazione del framework.....	94
5.4.3. Attuazione della gestione del rischio.....	95
5.4.4. Monitoraggio e riesame del framework	96
5.4.5. Miglioramento continuo del framework	96
5.5. Le attività critiche: la progettazione e l’informatizzazione.....	96
5.5.1. Come gestire i progetti: il masterplan e il diagramma di Gantt...	96
5.5.2. Il supporto informatico.....	99
5.6. Metodologie, standard internazionali e norme UNI	103

5.6.1. Standard specifici per il Data Protection	103
5.6.2. Standard per la sicurezza delle informazioni	104
5.6.3. Standard per il risk management	105
5.6.4. Standard per l'internal auditing	107
5.6.5. Standard per la prevenzione della corruzione	107
Capitolo 6 – Il Data protection impact assessment (DPIA)	
6.1. Il DPIA come modello giuridico	108
6.2. Il DPIA come processo "ordinario" di risk management	112
6.3. Definizione del contesto	115
6.3.1. Il contesto esterno ed interno	115
6.3.2. I documenti	116
6.3.3. I risk criteria	117
6.3.4. segue: i criteri per la misurazione del livello del rischio	117
6.4. La valutazione del rischio	118
6.5. Il trattamento del rischio: l'opzione della "mitigazione del rischio"	121
6.5.1. Le opzioni del risk treatment	121
6.5.2. La mitigazione del rischio	122
6.5.3. I presidi di controllo. Misure "organizzative" vs misure "tecno- logiche"	123
6.5.4. Consultazione preventiva	125
6.6. Consultazioni, reportistica e comunicazione	127
6.7. Il monitoraggio e il riesame	132
6.8. I data audit	132
6.8.1. A chi compete la responsabilità dei data audit	133
6.8.2. Come si svolgono i data audit	136
6.8.3. I metodi applicabili ai data audit	141
Glossario, acronimi e abbreviazioni	144

Indice delle tavole e delle figure

Capitolo 1 – Il sistema GDPR

Tavola 1 – Primi principi in materia di privacy	4
Figura 1 – Sintesi dell'evoluzione storica	6
Tavola 2 – Atti giuridici dell'Unione Europea	7
Figura 2 – Le categorie dei dati personali	9
Figura 3 – Adeguamento del quadro normativo nazionale alle disposi- zioni del Regolamento (UE) 2016/679	10
Figura 4 – Nozione di trattamento di dati	12
Figura 5 – Ambito di applicazione del GDPR	13
Figura 6 – I principi del trattamento dei dati (art. 5 GDPR)	14

Figura 7 – Il trattamento dei dati sensibili e giudiziari	18
Figura 8 – Condizioni per il trasferimento di dati a Paesi terzi	19
Figura 9 – Il codice di condotta	23
Figura 10 – Gli elementi del Data Breach	27
Figura 11 – Il sistema sanzionatorio	29
Figura 12 – Le linee guida del Gruppo “articolo 29”	33

Capitolo 2 – I diritti tutelati

Tavola 3 – Diritto alla protezione dei dati e diritto alla riservatezza.....	36
Figura 13 – Diritti degli interessati	37
Figura 14 – Limitazioni ai diritti degli interessati	38

Capitolo 3 – Conoscere e decidere

Figura 15 – Esempio di icone utilizzabili nell’informativa	51
Tavola 4 – Cookie Policy	53

Capitolo 4 – I soggetti e i ruoli

Figura 16 – Esempio di organigramma “data protection”	57
Figura 17 – Il Titolare del trattamento.....	59
Figura 18 – Proporzionalità delle misure tecniche ed organizzative.....	60
Tavola 5 – Il Responsabile del trattamento.....	62
Figura 19 – Nomina del Responsabile del trattamento.....	64
Tavola 6 – Compiti del DPO	66
Tavola 7 – Competenze e conoscenze del DPO.....	67
Figura 20 – Prerogative e doveri del DPO	69
Tavola 8 – Profili professionali: compiti principali	70
Figura 21 – I profili professionali della norma UNI 11697:2017	72
Tavola 9 – Requisiti per l’accesso ai profili professionali.....	72

Capitolo 5 – Il Data protection by design: progettare il trattamento dei dati

Tavola 10 – Categorie dei rischi da trattamento	74
Figura 22 – Mappatura dei rischi vs processi e strutture.....	76
Figura 23 – Ipotesi di sistema “data protection by design”	78
Figura 24 – Il Data protection by design.....	79
Figura 25 – Attività di controllo ed attori.....	82
Figura 26 – Processi, procedure e procedimenti amministrativi.....	85
Figura 27 – Grado di rischiosità rispetto all’adeguatezza del processo.....	86
Tavola 11 – Informazioni contenute nei registri delle attività di trattamento.....	88
Tavola 12 – Esempio di modello di registro delle attività di trattamento.....	90
Figura 28 – Il Framework.....	93
Tavola 13 – Le aree di progettazione del framework.....	94

Figura 29 – Il masterplan	97
Figura 30 – Gli step del masterplan.....	98
Tavola 14 – Esempio di funzionalità di un applicativo dedicato al data protection.....	100
Figura 31 – Cruscotti SSD: esempi di monitoraggio delle attività.....	100
Figura 32 – Esempio di gestione del registro dei trattamenti	101
Figura 33 – Il CoSO ERM	106

Capitolo 6 – Il Data protection impact assessment (DPIA)

Tavola 15 – Criteri per individuare trattamenti di dati ad alto rischio.....	109
Figura 34 – Il modello giuridico del DPIA	111
Figura 35 – Una concezione “operativa” del DPIA.....	114
Figura 36 – Criteri per la validità di un DPIA.....	115
Figura 37 – Gli output documentali del GDPR.....	116
Figura 38 – Matrice probabilità/impatto	118
Figura 39 – Rischi più comuni.....	119
Figura 40 – La fase della valutazione del rischio	121
Figura 41 – Misure organizzative e misure tecnologiche	125
Figura 42 – Le riunioni: fasi e ruoli.....	130
Figura 43 – Fasi dell’intervista.....	131
Figura 44 – Condizioni per lo sviluppo ed il riesame della DPIA.....	132
Tavola 16 – Specifiche del valutatore privacy.....	133
Tavola 17 – Raffronto tra DPO e Responsabile Internal audit	134
Figura 45 – Processo per la gestione di un programma di audit	137
Figura 46 – Processo di audit.....	138
Figura 47 – Il rapporto di audit	140
Tavola 18 – Metodi di audit.....	141



L'estratto che stai visualizzando
è tratto da un volume pubblicato su
ShopWKI - La libreria del professionista

[VAI ALLA SCHEDA PRODOTTO](#)