

INDICE

	<i>pag.</i>
Premessa	XI
Introduzione	XIII
Acronimi	XV
Guida alla lettura	XVII
1. I destinatari	XVII
2. Prerequisiti per la lettura	XVII
3. Ambito di trattazione	XVIII
4. Esclusioni	XIX
5. Suggerimenti e commenti	XIX
6. Struttura	XIX
6.1. Sintesi dei contenuti	XIX
6.2. Modelli e casi	XX
6.3. Note terminologiche	XX
6.4. Il ciclo PDCA	XXI

Capitolo 1

IL RUOLO SOGGETTIVO DEL DPO

1.1. L'Ufficiale della Protezione dei Dati – il DPO	1
1.2. Requisiti del DPO: le precisazioni delle Autorità e della Giurisprudenza	2
1.3. La nomina obbligatoria del DPO	5
1.3.1. La durata dell'incarico del DPO	9
1.3.2. L'attività principale dell'Organizzazione	9
1.4. DPO interno o esterno? Pro e contro delle due ipotesi	10
1.5. Le sanzioni delle Autorità di Controllo in caso di mancata nomina del DPO	11
1.6. Un unico DPO per più Organismi	12
1.7. Sintesi del “ <i>Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico</i> ”	14
1.8. Pubblicazione e comunicazione dei dati di contatto del DPO e la Sanzione dell'Autorità di Amburgo	18
1.9. DPO persona Giuridica: l'incarico deve essere conferito ad un lavoratore subordinato della stessa Società o, anche, ad un consulente esterno? La Sentenza del TAR Puglia n. 1468/2019 e l'intervento del Garante	21

	<i>pag.</i>
1.10. Il DPO può essere considerato un autorizzato ai sensi dell'art. 2-quattordicesimo Codice Privacy?	23
1.11. Nel caso in cui non sia nominato un DPO chi svolge le attività previste dall'art. 39 REG.EU. 2016/679?	28

Capitolo 2

LA POSIZIONE DEL DPO ALL'INTERNO DELL'ORGANIZZAZIONE

2.1. La tempestiva ed adeguata consultazione del DPO	31
2.1.1. Il dovere informativo del DPO verso gli Organi apicali dell'Organizzazione	32
2.2. Il DPO e il Titolare del trattamento	33
2.3. Il Referente Privacy quale <i>longa manus</i> del Titolare nel coinvolgimento del DPO	34
2.3.1. DPO e Ufficio privacy	35
2.4. Il Coinvolgimento del DPO con le altre funzioni dell'Organizzazione	36
2.4.1. Il DPO e la Funzione HR	36
2.4.2. Il DPO e la Funzione ICT	37
2.4.3. Il DPO, il Datore di lavoro e l'RSPP	38
2.4.4. Il DPO e le altre funzioni aziendali	39
2.4.5. Il DPO e gli altri Organi di controllo dell'Organizzazione	40
2.4.6. Il DPO e gli Auditor dei sistemi di gestione dell'Organizzazione	41
2.5. Le risorse messe a disposizione dal Titolare del trattamento al DPO: non sono solo risorse economiche	42
2.6. L'indipendenza del DPO	44
2.6.1. La gestione del budget del DPO	46
2.7. Il conflitto di interessi	46
2.7.1. L'incarico di DPO unitamente ad altri ruoli ... conflitto di interessi: la sanzione dell'Autorità belga	48
2.7.2. Il DPO può essere anche membro dell'Organismo di Vigilanza ai sensi del d.lgs. n. 231/2001?	49
2.8. Gli interessati e il DPO	51
2.9. Il parallelo tra i compiti del DPO e le misure a carico del Titolare del trattamento	52
2.10. Considerazioni conclusive sul ruolo del DPO	53

Capitolo 3

I COMPITI DEL DPO

3.1. Introduzione ai compiti del DPO	55
3.2. Il DPO informa e fornisce consulenza	57
3.2.1. Il DPO deve informare	58
3.2.2. Il DPO deve fornire consulenza	59
3.2.3. I controlli a capo del DPO	60

	<i>pag.</i>
3.3. L'attività di Audit del DPO	61
3.3.1. Il processo di Audit	61
3.3.2. I punti cruciali dell'audit all'attenzione del DPO	63
3.3.3. I vari tipi di audit	64
3.3.4. Alcune riflessioni sull'opportunità dell'Audit in capo al DPO	66
3.3.5. L'audit di conformità legislativa sui requisiti afferenti al DPO	68
3.3.6. Le tecniche per le interviste a supporto del DPO	69
3.3.7. Una alternativa all'audit: il monitoraggio	73
3.4. Il DPO e la formazione degli autorizzati	74
3.5. Il DPO sorveglia l'attribuzione di responsabilità	75
3.5.1. In particolare sulla matrice RACI	76
3.5.2. Il DPO e l'art. 32 "Sicurezza del trattamento" REG.EU. 2016/679	79
3.6. Il parere del DPO sulla valutazione d'impatto ai sensi dell'art. 35 REG.EU. 2016/679	80
3.7. Altre attività del DPO	81
3.7.1. Attività nei confronti degli interessati	81
3.7.1.1. Il DPO ed il <i>legal design</i>	82
3.7.2. Registro ed informativa agli interessati in relazione all'attività del DPO	83
3.7.3. Il ruolo del DPO in caso di Data Breach	83
3.7.3.1. Attività preliminare per un'efficiente gestione del Data Breach	84
3.7.3.2. Verifica del Data Breach	90
3.7.4. Il DPO: prassi e procedure	94
3.7.4.1. Il DPO ed il Modello Organizzativo Privacy	94
3.7.5. La gestione degli archivi del DPO	95
3.7.6. Il DPO e lo scadenziario	97
3.7.7. Il DPO e gli indicatori di processo	98
3.8. Considerazioni conclusive su come dare effettivo potere al DPO	98

Capitolo 4

L'ETICA DEL DPO

4.1. L'onorabilità del DPO	101
4.2. La riservatezza del DPO	102
4.3. La competenza del DPO	103
4.4. L'aggiornamento continuo del DPO	105
4.5. La consapevolezza del DPO	107
4.6. La correttezza e la lealtà del DPO	107
4.7. Il conflitto d'interesse del DPO	111
4.8. La comunicazione efficace del DPO	112

Capitolo 5

L'ATTIVITÀ DEL DPO E GLI STANDARD ISO 27701:2019 e BS 10012:2017

5.1.	Il DPO ed il sistema di gestione della protezione dei dati	115
5.2.	L'attività del DPO e gli standard internazionali	116
5.3.	Il DPO e le norme della famiglia ISO/IEC 27000	117
5.3.1.	Le norme della famiglia ISO/IEC 27000	118
5.3.2.	La funzione del DPO nelle norme della famiglia ISO/IEC 27000	119
5.4.	L'attività del DPO e la norma BS 10012:2017	122

Capitolo 6

**L'ACCOUNTABILITY DEL DPO RISPETTO
AL TITOLARE DEL TRATTAMENTO**

6.1.	Struttura dei documenti del DPO	127
6.2.	Modello – Nomina del DPO sia interno che esterno da parte del Vertice del Titolare del trattamento	128
6.3.	Modello – Relazione sull'opportunità della nomina del DPO	135
6.4.	Modello – Regolamento del DPO	137
6.5.	Modello – Flussi informativi verso il DPO	144
6.6.	Modello – Verbale di insediamento	149
6.7.	Modello – Verbale di “ordinaria amministrazione”	157
6.8.	Modello – Verbale mirato	180
6.9.	Modello – Verbale di “straordinaria amministrazione”	183
6.10.	Modello – Verbale di audit di conformità legislativa	188
6.11.	Modello – Verbale di audit di sistema di gestione della protezione dei dati personali	190
6.12.	Modello – Relazione annuale del DPO al vertice dell'Organizzazione	196
6.13.	Modello – Verbale di Data Breach	201
6.14.	Modello – Verbale di parere	206
6.15.	Modello – Verbale di valutazione PIA del DPO	207

Capitolo 7

**L'AGGIORNAMENTO IN CONCRETO DEL DPO: PROVVEDIMENTI
DELLE AUTORITÀ GARANTI E GIURISPRUDENZA**

7.1.	Provvedimenti n. 231 e 232 dell'11 dicembre 2019 dell'Autorità Garante italiana: determinazione della sanzione in base al fatturato della singola impresa e non in base al fatturato del gruppo imprenditoriale	212
7.2.	Provvedimento dell'autorità di controllo del Baden-Württemberg (LfDI Baden-Württemberg) del 30 giugno 2020: trattamento di dati personali per scopi pubblicitari senza il consenso	214
7.3.	Sentenza 40/17 del 29 luglio 2019 Corte di Giustizia dell'Unione Europea: qualificazione del Titolare del trattamento	215

	<i>pag.</i>
7.4. Provvedimento Autorità di controllo polacca – UODO – del 3 giugno 2020: mancata cooperazione della società	216
7.5. Provvedimento Autorità di controllo ungherese: e-mail aziendale	217
7.6. Provvedimento n. 138 e Provvedimento n. 143 del 9 luglio 2020 dell’Autorità Garante italiana: ordinanze ingiunzione nei confronti di Wind Tre S.p.A. e di Iliad Italia S.p.A.	218
7.7. Sentenza C-311/18, c.d. Schrems II, del 16 luglio 2020: abolizione del Privacy Shield	220
7.8. Provvedimento n. 86 del 14 maggio 2020 dell’Autorità Garante italiana: Data Breach dell’INPS	226
7.9. Provvedimento n. 99 del 10 giugno 2020 dell’Autorità Garante italiana: Data Breach Unicredit Banca	228
7.10. Provvedimento AEDPD n. 390/2019: utilizzo fogli di recupero	228
7.11. Provvedimenti n. 120, 118, 12 dell’Autorità Garante italiana 016: sanzioni ad Enti locali	229
7.12. Provvedimenti n. 126 del 2 luglio 2020 e n. 141 del 9 luglio 2020 dell’Autorità Garante italiana: illecito trattamento di dati sanitari	231
7.13. Cass. civ., Sez. VI-1, Ord., 20 agosto 2020, n. 17383: danno risarcibile	232
7.14. Ingiunzioni del CNIL in riferimento all’utilizzo di dati biometrici per la rilevazione delle presenze nei luoghi di lavoro	232
7.15. Corte di Giustizia dell’Unione europea – Sentenza del 11 novembre 2020 C-61/19 Orange România SA/ANSPDCP relativa alla manifestazione del consenso libero ed inequivocabile dell’interessato	233
7.16. Consiglio di Stato, Sez. III, 28 ottobre 2020, n. 6570: Diritto di accesso difensivo e tutela della riservatezza	234
7.17. Provvedimento Autorità di controllo spagnola – AEPD – del 10 settembre 2020: sanzione ad un partito politico per l’invio di email senza consenso	235
7.18. Sentenza Corte di Cassazione n. 34296/2020: costituisce reato l’accesso dell’ex socio al sistema informatico	236
7.19. Tribunale di Milano – I Sez. Civ. Ord. n. 44578/2020: accesso ai dati <i>post mortem</i> sul cloud	236
7.20. Provvedimento n. 90 del 11 marzo 2021 dell’Autorità Garante italiana: installazione sistema videosorveglianza da parte dell’Università degli Studi di Napoli	237
7.21. Provvedimento n. 144 del 15 aprile 2021 dell’Autorità Garante italiana: trattamento di dati sanitari e informazione scientifica	239
7.22. Provvedimento n. 136 del 15 aprile 2021 dell’Autorità Garante italiana: trattamento illecito di dati personali di dipendenti	240
7.23. Provvedimento n. 192 del 13 maggio 2021 dell’Autorità Garante italiana: ordinanza di ingiunzione nei confronti di Iren Mercato S.p.A.	242
7.24. Provvedimento n. 211 del 27 maggio 2021 dell’Autorità Garante italiana: Fascicolo Sanitario Elettronico e oscuramento dei dati sanitari	243

	<i>pag.</i>
7.25. Provvedimento n. 247 del 24 giugno 2021 dell’Autorità Garante italiana: Parere su uno schema di regolamento recante l’individuazione dei trattamenti di dati personali relativi a condanne penali e reati e delle relative garanzie appropriate ai sensi dell’articolo 2-octies, comma 2, del Codice	244
7.26. Cass. civ., Sez. I, Ordinanza, 11 novembre 2020-7 luglio 2021, n. 19270: la chiave elettronica dell’autovettura è un dato personale	246

Capitolo 8

LE SANZIONI

8.1. In particolare: i dati emersi in questi mesi	250
8.2. Uno sguardo alle sanzioni più emblematiche che sono state comminate, in Europa	253
8.3. Tabella delle sanzioni comminate	257
Bibliografia	259