

# INDICE

|   |      |      |
|---|------|------|
| <i>Prefazione di Guido Scorza</i>   | pag. | v    |
| <i>Introduzione di Rocco Panetta</i>  | pag. | xiii |
| <b>1. LA TEORIA DEL DPO</b>   | pag. | 1    |
| 1.1. L'introduzione del Data Protection Officer e le sue origini normative  | pag. | 1    |
| 1.2. Designazione del DPO tra facoltà e obbligo di legge  | pag. | 6    |
| 1.2.1. Casi in cui la nomina è obbligatoria   | pag. | 7    |
| 1.2.1.1. Autorità pubblica o organismo pubblico   | pag. | 10   |
| 1.2.1.2. Attività principali che consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala               | pag. | 13   |
| 1.2.1.3. Attività principali che consistono in trattamenti su larga scala di dati sensibili o di dati giudiziari  | pag. | 19   |
| 1.2.2. Facoltatività della nomina e DPO di associazioni rappresentative degli interessi di titolari e responsabili del trattamento                              | pag. | 20   |
| 1.2.3. ( <i>segue</i> ) l'obbligo di nomina del DPO per le autorità giudiziarie nell'esercizio delle loro funzioni <i>ex art. 2-sexiesdecies</i> Codice Privacy | pag. | 20   |
| 1.2.4. Casi residuali e <i>ratio</i> dell'impianto normativo  | pag. | 22   |
| 1.2.5. Obblighi di trasparenza  | pag. | 24   |
| 1.3. Semplificazioni per gruppi imprenditoriali o pluralità di soggetti pubblici  | pag. | 26   |
| 1.4. La nomina del DPO sulla base di un contratto di servizi (o in <i>outsourcing</i> ) – disciplina normativa  | pag. | 28   |
| 1.5. Competenze e conoscenze richieste per l'assolvimento della funzione di DPO   | pag. | 29   |
| 1.5.1. Certificazioni e formazione  | pag. | 31   |
| 1.5.2. Esperienza   | pag. | 37   |
| 1.5.3. Qualità e caratteristiche personali  | pag. | 38   |
| 1.6. Lo statuto legale del DPO nelle organizzazioni   | pag. | 39   |
| 1.6.1. Indipendenza del DPO   | pag. | 39   |
| 1.6.2. Conflitto di interessi   | pag. | 42   |
| 1.6.3. Posizionamento del DPO all'interno dell'organizzazione   | pag. | 45   |

|           |   |                |
|-----------|---|----------------|
| 1.6.4.    | Risorse adeguate e strutture di riferimento   | pag. 47        |
| 1.6.5.    | I poteri del DPO  | pag. 50        |
| 1.6.6.    | Profili formali   | pag. 52        |
| 1.7.      | I compiti e le funzioni del DPO   | pag. 53        |
| 1.7.1.    | Informazione e consulenza   | pag. 54        |
| 1.7.2.    | Sorveglianza attiva in materia di protezione dei dati   | pag. 56        |
| 1.7.3.    | Il DPO e la valutazione d'impatto sulla protezione dei dati (DPIA)                                    | pag. 57        |
| 1.7.4.    | Cooperazione con l'autorità di controllo e punto di contatto  | pag. 58        |
| 1.8.      | Il DPO orientato al rischio   | pag. 59        |
| <b>2.</b> | <b>LA PRATICA DEL DPO</b>   | <b>pag. 63</b> |
| 2.1.      | I principi di <i>Accountability</i> e <i>Privacy by design</i> e <i>by default</i> e il ruolo del DPO | pag. 63        |
| 2.1.1.    | Il principio di <i>Accountability</i>   | pag. 63        |
| 2.1.2.    | Il principio di <i>Privacy by-design</i> e <i>by-default</i>  | pag. 65        |
| 2.1.3.    | Il ruolo del DPO nel garantire il rispetto della <i>privacy by design</i>                             | pag. 67        |
| 2.2.      | I compiti preliminari di un DPO: piano di lavoro e mappatura  | pag. 70        |
| 2.3.      | La predisposizione e gestione del registro dei trattamenti  | pag. 74        |
| 2.3.1.    | L'obbligatorietà della tenuta del registro  | pag. 77        |
| 2.3.2.    | La tenuta del registro e il ruolo del DPO   | pag. 81        |
| 2.4.      | Il ruolo da 'consulente' del DPO  | pag. 84        |
| 2.5.      | Il DPO e la Valutazione d'Impatto sulla Protezione dei Dati   | pag. 87        |
| 2.5.1.    | Misure di gestione e minimizzazione dei rischi  | pag. 95        |
| 2.6.      | Il DPO e la gestione dei <i>Data Breach</i>   | pag. 103       |
| 2.6.1.    | L'analisi dei rischi in caso di <i>data breach</i>  | pag. 107       |
| 2.6.2.    | Tipologie di violazione dei dati personali  | pag. 108       |
| 2.6.2.1.  | Trattamenti elettronici dei dati  | pag. 109       |
| 2.6.2.2.  | Trattamenti cartacei dei dati   | pag. 110       |
| 2.6.3.    | Processo di gestione delle violazioni dei dati personali  | pag. 111       |
| 2.6.3.1.  | Segnalazione o rilevazione della violazione di dati personali   | pag. 112       |
| 2.6.3.2.  | Rilevazione degli eventi di violazione dei dati personali e valutazione                               | pag. 113       |
| 2.6.3.3.  | Notifica e Comunicazione  | pag. 115       |
| 2.6.4.    | L'iscrizione del <i>data breach</i> nel registro delle violazioni                                     | pag. 117       |
| 2.6.5.    | Obblighi specifici a carico dei fornitori esterni di servizi  | pag. 118       |

---

|          |  |          |
|----------|--|----------|
| 2.7.     | Il DPO e la gestione delle richieste di esercizio dei diritti da parte degli interessati | pag. 119 |
| 2.7.1.   | Gli obblighi del titolare e l'identificazione dell'interessato                           | pag. 119 |
| 2.7.2.   | I diritti riconosciuti agli interessati dal Regolamento (UE) 2016/679                    | pag. 125 |
| 2.7.2.1. | Diritto di accesso   | pag. 125 |
| 2.7.2.2. | Diritto di rettifica   | pag. 126 |
| 2.7.2.3. | Diritto alla cancellazione e diritto all'oblio   | pag. 126 |
| 2.7.2.4. | Diritto alla limitazione del trattamento   | pag. 128 |
| 2.7.2.5. | Notifica di rettifiche, cancellazioni o limitazioni del trattamento                      | pag. 128 |
| 2.7.2.6. | Diritto alla portabilità dei dati  | pag. 129 |
| 2.7.2.7. | Diritto di opposizione   | pag. 134 |
| 2.7.2.8. | Diritto a non essere sottoposti a processi decisionali automatizzati                     | pag. 135 |
| 2.7.3.   | Le limitazioni all'esercizio dei diritti   | pag. 137 |
| 2.7.4.   | La procedura di gestione delle richieste di esercizio dei diritti                        | pag. 138 |
| 2.8.     | Il DPO nei rapporti con l'Autorità Garante per la Protezione dei Dati Personali          | pag. 142 |
| 2.8.1.   | Prima dell'ispezione dell'Autorità   | pag. 145 |
| 2.8.2.   | Durante l'investigazione dell'Autorità   | pag. 146 |
| 2.9.     | Il ruolo del DPO nelle attività di <i>audit</i>  | pag. 148 |
| 2.9.1.   | Le tipologie di <i>audit</i> e il ruolo del DPO  | pag. 150 |
| 2.9.2.   | Le modalità di svolgimento degli <i>audit</i>  | pag. 152 |
| 2.9.3.   | Conclusione dell' <i>audit</i> e reportistica  | pag. 153 |
| 3.       | <b>LE 5 SFIDE CHE ATTENDONO IL FUTURO DEL DPO</b>  | pag. 157 |
| 3.1.     | DPO interno vs DPO in <i>outsourcing</i>   | pag. 161 |
| 3.2.     | Il DPO come funzione organica  | pag. 165 |
| 3.3.     | DPO di gruppo vs DPO per giurisdizione   | pag. 170 |
| 3.4.     | Il ruolo delle certificazioni  | pag. 173 |
| 3.5.     | La responsabilità del DPO  | pag. 176 |

