

INDICE

1. LA NOMINA DEL DPO

di Andrea Maggipinto

1.1. Identikit del DPO	pag.	9
1.2. Profilo del DPO. Requisiti. Certificazioni	pag.	13
1.3. Indipendenza e assenza di conflitti di interesse	pag.	15
1.3.1. Indipendenza	pag.	16
1.3.2. Conflitto di interesse	pag.	17
1.4. I compiti del DPO	pag.	18
1.5. Pubblicazione e comunicazione dei dati di contatto del DPO	pag.	19
1.6. Durata dell'incarico. Revoca	pag.	20
1.6.1. Durata dell'incarico	pag.	20
1.6.2. Cessazione dall'incarico. Revoca e rinuncia	pag.	21

2. IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO E I CONTROLLI DEL DPO

di Pietro Calorio

2.1. Premessa e note generali	pag.	23
2.2. Il ruolo del DPO	pag.	27
2.3. I controlli formali	pag.	27
2.3.1. Modalità di tenuta del registro	pag.	27
2.3.2. Struttura del registro	pag.	28
2.3.3. Data di emissione e di aggiornamento	pag.	29
2.3.4. Nomi e dati di contatto (Titolare, Responsabile, Rappresentante, DPO)	pag.	32
2.4. I controlli sostanziali	pag.	34
2.4.1. Finalità del Trattamento	pag.	34
2.4.2. Basi giuridiche del Trattamento	pag.	35
2.4.3. Categorie di Interessati	pag.	36
2.4.4. Categorie di Dati Personali	pag.	37
2.4.5. Categorie di destinatari	pag.	39
2.4.6. Trasferimenti verso paesi terzi e organizzazioni internazionali	pag.	40
2.4.7. Termini ultimi di cancellazione	pag.	41
2.4.8. Misure di sicurezza	pag.	42
2.4.9. Informazioni aggiuntive	pag.	44

3. LA CORRETTA INDIVIDUAZIONE DEI RUOLI: TITOLARE E RESPONSABILE

di Stefano Ricci, Andrea Michinelli

3.1. Concetti generali	pag.	47
------------------------	------	----

3.2. Il cambio di ottica: dalla nomina a Responsabile esterno per il Trattamento dei dati all'accordo per il Trattamento dei dati	pag. 48
3.3. La differenza tra Titolare e Responsabile del Trattamento	pag. 48
3.4. Contenuti dell'accordo per il Trattamento dei Dati personali / <i>data processing agreement</i> (ex art. 28 del GDPR)	pag. 50
3.5. Il Responsabile ulteriore ex art. 28 co. 2 e 4 del GDPR	pag. 55
3.6. Codici di condotta ex art. 28 co. 5 del GDPR e le clausole contrattuali tipo ex art. 28 co. 6, 7 e 8 del GDPR	pag. 56
3.7. Il ruolo del DPO nella valutazione dei DPA in relazione agli aspetti contrattuali col Responsabile	pag. 56
3.8. Profili sanzionatori	pag. 56

4. IL DPO E LA VERIFICA DELLE INFORMATIVE

di *Andrea Michinelli, Gianmaria Le Metre*

4.1. Premessa	pag. 59
4.2. Principio di trasparenza art. 12 GDPR applicato all'informativa	pag. 59
4.3. Contenuti e modalità di comunicazione dell'informativa	pag. 61
4.4. Accountability: dimostrare online la miglior trasparenza informativa possibile	pag. 65
4.5. Le eccezioni all'obbligo di rendere l'informativa	pag. 66
4.6. Tempistiche nella resa dell'informativa e delle sue modificazioni	pag. 68
4.7. Sanzioni applicabili	pag. 69

5. IL DPO E LE MISURE TECNICHE ORGANIZZATIVE: ATTIVITÀ DI VERIFICA INFORMATICA NEI CONFRONTI DELL'AZIENDA O DEL FORNITORE ESTERNO

di *Marco Tullio Giordano*

5.1. Premessa	pag. 71
5.2. Fondamenti normativi: l'art. 39 comma 1, lettera b), gli artt. 24 e 25, l'art. 32. L'art. 28 comma 3 lettere c), e), f) ed h) del GDPR	pag. 72
5.3. La verifica del livello di sicurezza adeguato al rischio	pag. 75
5.4. Pseudonimizzazione e cifratura dei Dati Personali	pag. 76
5.5. Verifica della capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Trattamento	pag. 77
5.6. Verifica della capacità di ripristinare tempestivamente la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico. Misure di <i>business continuity</i> e <i>disaster recovery</i>	pag. 79
5.7. Verifica della presenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento	pag. 80
5.8. Verifica della presenza di misure volte all'informazione ed alla formazione degli autorizzati al Trattamento: il regolamento aziendale sull'utilizzo delle risorse informatiche	pag. 81
5.9. Verifica e monitoraggio delle misure tecniche ed organizzative poste in essere dai processor del Titolare	pag. 81
5.10. Sanzioni applicabili	pag. 82

6. IL DPO E IL RISCONTRO ALL'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

di *Andrea Michinelli*

6.1. Premessa	pag.	83
6.2. I diritti esercitabili da parte dell'Interessato (artt. 15-22 GDPR)	pag.	84
6.3. La trasparenza (art. 12 GDPR) nell'esercizio dei diritti dell'Interessato	pag.	91
6.3.1. La richiesta dell'Interessato	pag.	91
6.3.2. Il riscontro/notifica alla richiesta dell'interessato	pag.	92
6.3.3. Ulteriori notifiche del Titolare	pag.	93
6.4. Le limitazioni all'esercizio dei diritti	pag.	93
6.5. Il caso degli Interessati minorenni, deceduti o dei terzi richiedenti	pag.	94
6.6. Sanzioni applicabili	pag.	95

7. IL DPO E LA FORMAZIONE

di *Gianluigi Sironi*

7.1. La norma: art. 38 GDPR	pag.	97
7.2. La norma sulla formazione UNI ISO 29990: 2011	pag.	98
7.3. Le indicazioni del CNIL del 2011	pag.	98
7.4. Le fasi del processo formativo	pag.	98
7.5. La sensibilizzazione del personale: i suggerimenti di ICO	pag.	100
7.6. La formazione del DPO	pag.	101

8. IL DPO IN CASO DI DATA BREACH

di *Giuseppe Vaciago, Nicole Monte*

8.1. Premessa	pag.	103
8.2. Requisiti della notifica	pag.	104
8.3. Procedura di notifica	pag.	105
8.3.1. Matrice RACI	pag.	106
8.4. Il ruolo del DPO	pag.	107
8.4.1. Abilità e competenza	pag.	107
8.4.2. Punto di raccordo con l'Autorità Garante per la Protezione dei Dati Personali	pag.	107
8.5. La notifica all'Autorità Garante per la Protezione dei Dati Personali	pag.	108

9. LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

di *Stefano Ricci, Antonio Perrini*

9.1. La Valutazione di Impatto	pag.	113
9.2. Quando fare la Valutazione di Impatto	pag.	114
9.2.1. Il concetto di rischio elevato	pag.	116
9.2.2. Il concetto di elevato rischio insito e di larga scala	pag.	116
9.2.3. Altri casi di Valutazione di Impatto obbligatoria: l'elenco pubblicato dall'Autorità Garante per la Protezione dei Dati Personali e i criteri presenti nelle Linee Guida WP248	pag.	117

9.2.4	Se il Trattamento presenta un rischio elevato: casi di eccezione all'obbligo di svolgere una Valutazione di Impatto	pag. 122
9.2.5	Se il Trattamento presenta un rischio elevato: obbligo di svolgere e rivalutare periodicamente la Valutazione di Impatto	pag. 123
9.3.	Come fare la Valutazione di Impatto	pag. 124
9.3.1.	Come fare la DPIA: il contenuto ed il metodo	pag. 124
9.3.2.	Soggetti coinvolti con particolare riferimento al ruolo del DPO	pag. 127
9.4.	Le sanzioni	pag. 128

10. DPO E RAPPORTI CON L'AUTORITÀ DI CONTROLLO

di **Pietro Calorio**

10.1.	Premessa e annotazioni generali	pag. 129
10.2.	La questione del segreto	pag. 130
10.3.	Il DPO nell'ambito dei compiti e dei poteri dell'Autorità	pag. 133
10.3.1.	Compiti/poteri consultivi: la consultazione preventiva	pag. 133
10.3.2.	Poteri di indagine e correttivi	pag. 134

COLLABORATORI

Pietro Calorio, Avvocato in Torino. Fondatore dello Studio Legale Calorio-De Marcus. Consulente in materia di informatica giudiziaria e privacy (Certificati TÜV Italia - schema CDP in accordo alla ISO/IEC 17024:2012 - e CEPAS - profilo DPO secondo UNI 11697:2017). DPO nel settore pubblico (in particolare sanitario) e privato. Svolge attività di divulgazione e formazione su PCT e *data protection*. Presidente dell'associazione Sloweb (www.sloweb.org).

Marco Tullio Giordano, Avvocato in Milano, si occupa di diritto penale delle nuove tecnologie dal 2008, con particolare attenzione ai temi della *cybersecurity* e della *data protection*. È lead auditor 27001:2017 e DPO nel settore privato. Collabora con la cattedra di Informatica Giuridica dell'Università degli Studi di Milano ed è relatore di corsi di formazione su privacy e *cybercrimes*.

Gianmaria Le Metre, Avvocato in Bologna. Ha conseguito un *master* di II livello in Diritto della Proprietà Intellettuale con Just Legal Services (Milano). Collaboratore dello Studio Legale D'Amassa & Partners in materia di IP e di *privacy*.

Andrea Maggipinto, Avvocato in Milano, titolare dello studio legale AMLAW con *focus* in diritto delle nuove tecnologie, proprietà intellettuale

e *privacy*. Dottore di ricerca in informatica giuridica, arbitro in procedure *ex artt. 806 ss. c.p.c.*, esperto per la risoluzione delle controversie su nomi a dominio. Dal 2018 è certificato per il profilo professionale "*Data Protection Officer*" secondo la norma UNI 11697:2017.

Andrea Michinelli, Avvocato in Bologna. Cofondatore dello Studio Legale d'Ammassa & Partners. Certificato per il profilo professionale "*Data Protection Officer*" secondo la norma UNI 11697:2017, Consulente della Privacy e Privacy Officer secondo lo schema CDP TÜV SÜD, certificato CIPP/E e membro della IAPP (International Association of Privacy Professionals). Divulgatore e docente in corsi di formazione sulla *privacy*, nuove tecnologie e IP.

Nicole Monte, Avvocato in Milano dal 2014, *privacy* e *cybersecurity specialist*. È assegnista di ricerca presso il Politecnico di Torino ed è specializzata in diritto delle nuove tecnologie. Ha seguito numerosi casi di cybercrime ai danni di alcune importanti società nazionali e internazionali.

Antonio Perrini, Avvocato in Milano, si è laureato nel 2013 presso l'Università degli Studi di Milano-Bicocca con una tesi in Informatica Giuridica focalizzata sulle problematiche tecnico-giuridiche del documento informatico. Presta regolarmente consulenza a clienti italiani e internazionali in materia di protezione dei dati personali e di progetti di adeguamento al GDPR, con particolare attenzione alle tematiche di protezione dei dati personali nelle operazioni societarie.

Stefano Ricci, Avvocato in Milano, ha conseguito un PHD sui Global Privacy Standard all'Università degli Studi di Milano Bicocca ed è docente di informatica giuridica presso l'Università degli Studi dell'Insubria. È certificato per il profilo professionale "*Data Protection Officer*" secondo la norma UNI 11697:2017.

Gianluigi Sironi, Avvocato in Milano dal 2006. Ha conseguito la certificazione per il profilo professionale "*Data Protection Officer*" seconda la norma UNI 11697:2017. Svolge attività di consulenza in materia di *data protection* e di contenzioso di diritto civile.

Giuseppe Vaciago, Avvocato in Milano, esperto in diritto delle nuove tecnologie. Ha conseguito un PHD in Digital Forensics all'Università degli Studi di Milano Bicocca ed è docente di informatica giuridica presso l'Università degli Studi dell'Insubria dal 2007. È *lead auditor 27001:2017* e certificato per il profilo professionale "*Data Protection Officer*" secondo la norma UNI 11697:2017.