

SOMMARIO

PRESENTAZIONE	III
INDICE AUTORI	XIII
PARTE I – I PRINCIPI IN MATERIA DI TRATTAMENTO DEI DATI	
1. L'AMBITO DI APPLICAZIONE	
1.1. Introduzione.....	3
1.2. Ambito di applicazione materiale.....	3
1.3. Ambito di applicazione territoriale.....	4
1.3. Ambito di applicazione territoriale.....	9
2. IL RISPETTO DEI PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI	
2.1. Introduzione.....	16
2.2. Liceità, correttezza e trasparenza.....	16
2.3. Limitazione della finalità.....	16
2.4. Minimizzazione dei dati.....	20
2.5. Esattezza.....	22
2.6. Limitazione della conservazione.....	24
2.7. Integrità e riservatezza.....	24
2.7. Integrità e riservatezza.....	25
2.8. Responsabilizzazione o “accountability”.....	26
3. INDIVIDUAZIONE DELLE BASI GIURIDICHE PER IL TRATTAMENTO	
3.1. Premessa.....	29
3.1. Premessa.....	29
3.2. Il consenso.....	29
3.2. Il consenso.....	31
3.3. Necessità di esecuzione di un contratto.....	39
3.3. Necessità di esecuzione di un contratto.....	39
3.4. L'adempimento di un obbligo legale.....	41
3.4. L'adempimento di un obbligo legale.....	41
3.5. La salvaguardia di interessi vitali.....	41
3.5. La salvaguardia di interessi vitali.....	41
3.6. L'esecuzione di un compito di interesse pubblico.....	42
3.6. L'esecuzione di un compito di interesse pubblico.....	42
3.7. Il legittimo interesse.....	43
3.7. Il legittimo interesse.....	43
4. I DIRITTI DEGLI INTERESSATI	
4.1. Premessa.....	46
4.1. Premessa.....	46
4.2. Informazioni sul trattamento.....	46
4.2. Informazioni sul trattamento.....	47
4.3. Modalità di esercizio dei diritti dell'interessato.....	47
4.3. Modalità di esercizio dei diritti dell'interessato.....	50
4.4. I diritti dell'interessato.....	50
4.4. I diritti dell'interessato.....	52
4.5. Limitazioni all'esercizio dei diritti dell'interessato.....	52
4.5. Limitazioni all'esercizio dei diritti dell'interessato.....	67

PARTE II - GLI ADEMPIMENTI NELL'ORGANIZZAZIONE

5. IL DATA PROTECTION OFFICER O RESPONSABILE DELLA PROTEZIONE DEI DATI	73
5.1. Introduzione: la figura del DPO.....	73
5.2. Quando nominare un DPO	74
5.3. Come scegliere il DPO e chi nominare.....	79
5.4. Il ruolo del DPO all'interno dell'organizzazione del titolare o responsabile del trattamento	81
5.5. Funzione e compiti del	85
6. IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO	87
6.1. Premesse.....	87
6.2. La tenuta del registro: tra obbligo e opportunità	88
6.3. Il contenuto del registro	89
6.4. Modalità di raccolta, conservazione e aggiornamento delle informazioni	93
7. LA CONSERVAZIONE DEI DATI	95
7.1. Premesse.....	95
7.2. La data retention policy.....	96
7.3. ...E le altre procedure	98
7.4. L'informativa agli interessati.....	100
8. SISTEMA DI GESTIONE DELLA PROTEZIONE DATI (SGPD) IN AZIENDA	101
8.1. Introduzione	101
8.2. Cosa è un SGPD	103
8.3. Componenti di base di un SGPD per conformità al GDPR.....	110
8.4. Considerazioni sul piano di implementazione di un SGPD.....	132
8.5. Rapporti del team privacy in azienda.....	135
8.6. SGPD in uso	140
8.7. Aggiornamento del SGPD	149
8.8. Conclusioni	151
9. DIRITTO DEL LAVORO E PRIVACY	154
9.1. Il rapporto di lavoro tra potere di controllo e tutela della riservatezza	154
9.2. Il quadro normativo	155
9.3. Il controllo diretto dei dipendenti	156
9.4. I controlli a distanza	161
9.5. Le garanzie procedurali	163
9.6. Gli strumenti del controllo a distanza.....	164
9.7. I controlli difensivi	165
9.8. Il trattamento dei dati personali nel rapporto di lavoro.....	166

9.9.	Finalità del Codice e definizioni	167
9.10.	Ruolo e obblighi del datore di lavoro	171
9.11.	Diritto di accesso ed azioni del lavoratore	174
9.12.	Gli ambiti di intervento del Garante Privacy.....	175
9.13.	Internet e Posta elettronica.....	176
9.14.	I dati biometrici del lavoratore.....	177
9.15.	Il necessario coordinamento tra il Codice Privacy e le altre norme del diritto del lavoro	178
9.16.	La tutela dei dati personali dei lavoratori ai tempi del Covid-19	179

PARTE III - VALUTAZIONE E GESTIONE DEL RISCHIO

10. PRIVACY BY DESIGN E BY DEFAULT	183
10.1. Premessa.....	183
10.2. Il principio di privacy by default.....	185
10.3. Il principio di privacy by design	188
10.4. Privacy engineering: le strategie per incorporare la privacy nel	192
10.5.	196
11. LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI.....	204
11.1. Cos'è e quando serve la DPIA.....	204
11.2. Ruoli e contenuti	206
11.3. La consultazione preventiva	211
12. LE MISURE DI SICUREZZA E CYBERSECURITY	213
12.1. Principi generali - misure tecniche ed organizzative.....	213
12.2. Adeguatezza delle misure di sicurezza	217
12.3. Gli standard ISO	218
12.4. Cybersecurity.....	219
13. CODICI DI CONDOTTA E CERTIFICAZIONI	226
13.1. Premessa.....	226
13.2. I codici di condotta	226
13.3. Le forme di autoregolamentazione dalla previgente disciplina del Codice Privacy al GDPR	227
13.4. Gli Organismi di monitoraggio	231
13.5. Le certificazioni	233
14. DATA BREACH	235
14.1. Premessa.....	235
14.2. Gli elementi della violazione e criteri per determinare l'effettiva conoscenza.....	236
14.3. Obblighi di notifica	237
14.4. La comunicazione agli interessati.....	243

14.5. Le procedure interne per la gestione dei	245
--	-----

PARTE IV - I RAPPORTI CON I TERZI

15. I RAPPORTI CON I TERZI	251
15.1. Premessa.....	251
15.2. I ruoli privacy.....	252
15.3. Obblighi e responsabilità	266
15.4. Gli accordi.....	268
16. I TRASFERIMENTI TRANSFRONTALIERI DI DATI	279
16.1. Principi fondamentali e disciplina generale in materia di trasferimenti transfrontalieri di dati.....	279
16.2. Quando è legittimo il trasferimento dei dati personali all'estero?	280
16.3. I nuovi scenari post brexit.....	294

PARTE V - I RAPPORTI CON LE AUTORITÀ

17. I POTERI CORRETTIVI DELLE AUTORITÀ DI CONTROLLO E LE SANZIONI	299
17.1. Premessa.....	299
17.2. I poteri correttivi delle autorità di controllo	299
17.3. Le sanzioni pecuniarie	302
17.4. Le sanzioni e i reati previsti dal codice privacy.....	307

PARTE VI - IL TRATTAMENTO DEI DATI PERSONALI IN

18. SETTORE SANITARIO PARTE I: FINALITÀ DI CURA E PRIVACY	313
18.1. Il dato sanitario	313
18.2. E-health	317
18.3. I dispositivi medici o elettromedicali.....	323
19. SETTORE SANITARIO PARTE II: RICERCA MEDICA E PRIVACY	325
19.1. Introduzione: la ricerca	325
19.2. La ricerca medica, biomedica e epidemiologica	325
19.3. I dati genetici e la ricerca clinica	333
19.4. Utilizzo successivo dei dati di ricerca	338
19.5. I registri pubblici e privati per il monitoraggio (.....	339
20. TRATTAMENTO DATI BANCARI E FINANZIARI	343
20.1. Introduzione	343

20.2.	Ambito di applicazione del trattamento dei dati finanziari.....	344
20.3.	Dritti degli interessati e portabilità dei dati	346
20.4.	Principali Provvedimenti e Linee Guida dell'Autorità Garante per la protezione dei dati personali	349
20.5.	Payment Service Directive 2 (PSD2) e l'impatto sul trattamento dei dati bancari	354
21.	DIRITTO ASSICURATIVO E PRIVACY	361
21.1.	Introduzione	362
21.2.	Reti distributive, periti ed altri collaboratori dell'impresa	362
21.3.	Data Governance assicurativa: definizione di un sistema di trasmissione delle informazioni efficace	367
21.4.	Il trattamento dei dati giudiziari in ambito assicurativo	369
21.5.	Il trattamento dei dati di salute in ambito assicurativo: assunzione e gestione dei sinistri	371
21.6.	Sistema di prevenzione delle frodi (responsabilità civile auto)	373
21.7.	Intelligenza artificiale, big data e settore assicurativo.....	374
21.8.	Diritto di accesso ai dati personali e gestione della fase pre-contenziosa	379
21.9.	Antiriciclaggio	380
21.10.	Trattamento dati all'interno delle aree riservate.....	382
21.11.	384
22.	MEDIA & PRIVACY	386
22.1.	Premessa.....	386
22.2.	La disciplina applicabile	386
22.3.	La tutela dell'immagine in ambito media.....	388
22.4.	I requisiti privacy in ambito media.....	392
22.5.	I diritti dell'interessato	397
22.6.	Conclusioni: la centralità del bilanciamento di interessi.....	399
23.	LA PRIVACY NELLE COMUNICAZIONI ELETTRONICHE	400
23.1.	L'evoluzione della disciplina delle comunicazioni elettroniche.	400
23.2.	L'ambito di applicazione del titolo X del codice della privacy...	403
23.3.	Informazioni e dati raccolti nei riguardi del contraente e dell'utente	406
23.4.	Marketing diretto e	410
23.5.	Informazioni, conservazione dei dati e sicurezza	413
23.6.	Il regolamento ePrivacy: il futuro (prossimo) della normativa sulle comunicazioni elettroniche	414
24.	SHARING ECONOMY	422
24.1.	Il ruolo della privacy nelle piattaforme della sharing economy	422
24.2.	L'effettività del consenso dell'utente al trattamento	427
24.3.	La raccolta, condivisione e trasferimento extra-UE dei dati personali	430
24.4.	La declinazione dei diritti privacy nella	439

25. LA PROTEZIONE DEI DATI PERSONALI NEL SETTORE DEI GIOCHI PUBBLICI	
	444
25.1. La disciplina dei giochi pubblici in Italia. Il gioco su rete fisica e il gioco a distanza	444
25.2. Gioco pubblico e tutela dei minori.....	451
25.3. Il	454
25.4. La normativa antiriciclaggio nel settore dei giochi e la tutela dei dati personali dei giocatori	463
PARTE VII - FORMULARIO	
26. INFORMAZIONI E DIRITTI DELL'INTERESSATO	
	475
26.1. Informazioni sui dati personali presso l'interessato (art. 13 GDPR) - informativa aziende private	477
26.2.	480
26.3. Informazioni sui dati personali (art. 13 GDPR) - informativa enti pubblici.....	482
26.4. Informazioni sui dati personali raccolti presso soggetti diversi dall'interessato (art. 14 GDPR) - informativa enti pubblici	484
26.5. Privacy policy per aziende	486
26.6. Cookie policy	489
26.7. Informativa e consenso per newsletter	492
26.8.	494
26.9. Informativa sui dati personali per dipendenti e collaboratori....	495
26.10. Informativa privacy per rilevazione temperatura corporea (emergenza COVID-19).....	498
26.11. Informativa sui dati personali di soggetti che accedono ai locali e agli uffici (emergenza COVID-19)	500
26.12. Esercizio del diritto di accesso in materia di protezione dei dati personali (art. 15 GDPR)	502
26.13. Esercizio di diritti in materia di protezione dei dati personali - Modello Garante Privacy	503
26.14. Esercizio di diritti in materia di protezione dei dati personali relativi a persona deceduta.....	505
26.15. Esercizio del diritto alla portabilità in materia di protezione dei dati personali	508
26.16. Istanza di esercizio del diritto alla portabilità dei dati	509
26.17. Riscontro ad istanza diritto alla portabilità dei dati.....	510
26.18. Istanza di esercizio del diritto di rettifica ed integrazione dei dati	511
26.19. Procedura aziendale per i diritti degli interessati	512
26.20. Reclamo ex art. 77 del Regolamento (UE) 2016/679	513
27. FIGURE E RUOLI	
	515
27.1. Accordo di contitolarità sui trattamenti di dati personali.....	516
27.2. Richiesta del contenuto dell'accordo di contitolarità	521
27.3. Riscontro a richiesta di accesso al contenuto dell'accordo di contitolarità	522

27.4.	Accordo per il trattamento dei dati da parte del responsabile esterno	523
27.5.	Documentazione delle scelte per la nomina del RPD o DPO (scelta di dotarsi di un DPO).....	530
27.6.	Documentazione delle scelte per la nomina del RPD o DPO (scelta di non dotarsi di un DPO).....	531
27.7.	Schema di atto di designazione del RDP esterno	532
27.8.	Schema di atto di designazione del RPD interno	535
27.9.	Dichiarazione sostitutiva di atto di notorietà - Insussistenza di conflitto di interesse del RPD (Enti pubblici).....	539
27.10.	Istruzioni per comunicazione del nominativo del DPO o RPD al Garante	540
27.11.	Segnalazione di ordine di priorità	541
27.12.	Verifica e aggiornamento delle informative privacy con integrazione del DPO o RPD	542
27.13.	Designazione componenti team del RPD o DPO	543
27.14.	Nomina componenti rete addetti di supporto al RPD o DPO ...	545
27.15.	Fac simile di relazione sintetica delle attività del RPD o DPO	546
27.16.	Atto di nomina amministratore di sistema.....	547
27.17.	Fac simile di relazione annuale attività dell'Amministratore di Sistema e verbale di verifica del Titolare sulle attività dell'Amministratore di Sistema	549
27.18.	Fac simile di designazione di referente interno	551
27.19.	Autorizzazione ai dipendenti al trattamento dei dati	553
27.20.	Istruzioni autorizzato individuale.....	555
28.	REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO	
		557
28.1.	Garante Privacy - Registri semplificati delle attività dei trattamenti per le PMI	558
28.2.	Registri delle attività di trattamento - Fac simile registro delle attività di trattamento del titolare (strutture complesse).....	559
28.3.	Registri delle attività di trattamento - Fac simile registro delle attività di trattamento del responsabile (strutture complesse) .	560
29.	VALUTAZIONE DI IMPATTO PRIVACY	
		561
29.1.	Richiesta di parere sulla valutazione di impatto privacy o Data Protection Impact Assessment (DPIA).....	562
29.2.	Scheda descrittiva allegata alla richiesta di parere al Responsabile della protezione dei dati personali sulla valutazione di impatto privacy o Data Protection Impact Assessment (DPIA)	563
29.3.	Parere sulla valutazione di impatto privacy o Data Protection Impact Assessment (DPIA).....	565
29.4.	Riscontro alla richiesta di parere di valutazione impatto privacy	567
30.	VIOLAZIONE DEI DATI	
		568
30.1.	Procedura di data breach	569

SOMMARIO

30.2.	Costituzione di un Punto di contatto informazione su data breach	573	
30.3.			574
30.4.	Nomina Unità di crisi – Data breach	575	
30.5.	Violazione di dati personali- modello di notifica al Garante	576	
30.6.	Comunicazione di violazione di dati personali all'interessato ..	577	
30.7.	Registro delle violazioni dei dati	578	
31.	VIDEOSORVEGLIANZA		
		580	
31.1.	Informazioni per esteso in relazione all'utilizzo di sistemi di videosorveglianza (art. 13 del GDPR)	581	
31.2.	Autorizzazione individuale ai dipendenti al trattamento dei dati in relazione a impianti di videosorveglianza.....	583	
INDICI			
INDICE CASI		587	
INDICE FORMULE		590	
INDICE ANALITICO		592	