

a cura di Giovanni Comandé e Gianclaudio Malgieri

GUIDA AL TRATTAMENTO E ALLA SICUREZZA DEI DATI PERSONALI

Le opportunità e le sfide del Regolamento Ue
e del Codice italiano riformato

Chiuso in redazione il 10 aprile 2019

ISBN 978-88-324-9235-4

GRUPPO24ORE

© 2019 Il Sole 24 ORE S.p.A.

Sede legale e amministrazione: via Monte Rosa, 91 – 20149 Milano

Redazione: via Monte Rosa, 91 – 20149 Milano

Per informazioni: Servizio Clienti 02.30.300.600-06.30.300.600

Fax 02.3022.5400-06.3022.5400

e-mail servizioclienti.libri@ilsole24ore.com

Fotocomposizione: Emmegi Group via F. Confalonieri, 36 Milano

Stampa: Rotolito Lombarda, via Sondrio, 3 - 20096 Seggiano di Pioltello (MI)

Seconda edizione: aprile 2019

Tutti i diritti sono riservati.

I testi e l'elaborazione dei testi, anche se curati con scrupolosa attenzione, non possono comportare specifiche responsabilità dell'Editore per involontari errori e/o inesattezze; pertanto il lettore è tenuto a controllare l'esattezza e la completezza del materiale utilizzato.

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633. Le riproduzioni effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da EDISER Srl, Società di servizi dell'Associazione Italiana Editori, attraverso il marchio CLEARedi, Centro licenze e Autorizzazioni Riproduzioni Editoriali, Corso di Porta Romana n. 108 - 20122 Milano.

Informazioni: www.clearedi.org.

Indice

	Prefazione	pag. XI
1.	Il diritto alla protezione dei dati personali: introduzione, struttura e principi generali	
1.1	Inquadramento normativo: fonti primarie, fonti secondarie e il “ <i>Data Protection Framework</i> ”	» 2
1.2	Il passaggio dalla disciplina del D.Lgs. 196/2003 al Regolamento e al D.Lgs. 101/2018	» 3
1.3	Ambito di applicazione materiale: il trattamento di dati personali	» 8
1.3.1	La definizione di “dato personale” e il problema dell’identificabilità	» 9
1.3.2	La definizione di trattamento di dati personali e la variabile dell’automatizzazione	» 10
1.3.3	Casi di esclusione dall’ambito materiale	» 11
1.4	Ambito di applicazione territoriale: l’ampliamento rispetto alla Direttiva.....	» 12
1.5	Altre definizioni: i soggetti coinvolti nel trattamento. Cenni e rinvio	» 13
1.6	La nuova figura del <i>Data Protection Officer</i> : requisiti, ruolo, posizione, compiti	» 14
1.7	I principi generali del Regolamento alla base del trattamento di dati personali	» 19
1.7.1	Il principio di liceità, correttezza e trasparenza	» 19
1.7.2	Il principio di limitazione della finalità	» 20
1.7.3	Il principio di minimizzazione dei dati	» 21
1.7.4	Il principio di esattezza	» 21
1.7.5	Il principio di limitazione della conservazione	» 22
1.7.6	Il principio di integrità e riservatezza	» 22
1.7.7	Il principio di <i>accountability</i>	» 23
1.8	Dati anonimi e dati pseudonimizzati	» 23
1.9	Tecniche di Anonimizzazione e Pseudonimizzazione	» 26
1.9.1	Tecniche di Pseudonimizzazione	» 27
1.9.2	Tecniche di Anonimizzazione.....	» 28

	1.9.3 Una metodologia per la gestione del rischio di <i>privacy</i>	»	33
1.10	I soggetti e le responsabilità nel nuovo Regolamento	»	34
1.11	Casi di liceità del trattamento dei dati personali.....	»	39
	1.11.1 Premessa	»	39
	1.11.2 La legittimità del trattamento ai sensi dell'art. 6.....	»	39
	1.11.3 Liceità del trattamento di particolari categorie di dati	»	40
	1.11.4 Le specificazioni del Sistema italiano sulle basi giuridiche del trattamento	»	42
1.12	Categorie di dati personali e tutela <i>sui generis</i>	»	43
	1.12.1 Le categorie sensibili e le ragioni di una tutela specifica	»	43
	1.12.2 I dati biometrici e il caso delle fotografie	»	44
	1.12.3 I dati relativi alla salute	»	45
1.13	Le caratteristiche del consenso al trattamento	»	46
	1.13.1 La valida acquisizione del consenso	»	46
	1.13.2 L'acquisizione del consenso da parte dei minori d'età	»	48
2.	I diritti dei soggetti interessati nel trattamento dei dati personali e le limitazioni (nazionali) a tali diritti		
2.1	I diritti dell'interessato nel Regolamento: tra novità ed obblighi corrispondenti	»	51
	2.1.1 Introduzione ai diritti dell'interessato: quadro generale.....	»	51
2.2	Diritto di revocare il consenso.....	»	53
2.3	Il diritto di ricevere informazioni e il diritto d'accesso.....	»	53
	2.3.1 Il diritto di ricevere informazioni	»	54
	2.3.2 Il diritto d'accesso	»	57
2.4	Il diritto alla rettifica	»	59
2.5	Diritto all'oblio.....	»	59
2.6	Il diritto alla limitazione del trattamento.....	»	63
2.7	Il diritto alla portabilità dei dati personali.....	»	64
2.8	Il diritto di opposizione	»	67
2.9	Profilazione automatizzata e diritto a non esserne soggetti	»	68
2.10	Le limitazioni alla portata degli obblighi e dei diritti.....	»	72
	2.10.1 L'Art. 23 GDPR e il rinnovato Codice sui dati personali	»	72
	2.10.2 Il coordinamento con la normativa in materia di <i>Whistle- blowing</i>	»	73
3.	Gli obblighi del titolare e del responsabile del trattamento: tecniche di attuazione e possibili sanzioni		
3.1	Gli adempimenti previsti dal regolamento: quadro generale, i re- gistri.....	»	75

3.1.1	Il nuovo obbligo di tenuta del registro delle attività di trattamento di dati personali	»	78
3.2	Gli adempimenti del Regolamento in tema di “ <i>data breach</i> ” e “ <i>data breach notification</i> ”	»	79
3.3	La Valutazione d’impatto sulla protezione dei dati personali (DPIA)	»	84
3.3.1	Le origini della Valutazione d’impatto (<i>Impact Assessment</i>)	»	84
3.3.2	Il <i>Data Protection Impact Assessment</i> nel Regolamento: l’art. 35	»	85
3.3.3	La consultazione preventiva in caso di rischio elevato senza contromisure	»	92
3.4	Dalla DPIA alle contromisure tecniche	»	93
3.4.1	La valutazione del rischio	»	94
3.4.2	La scelta delle contromisure tecniche ed organizzative: un approccio metodologico	»	95
3.4.3	Le fasi di valutazione del rischio secondo le linee guida ENISA	»	96
3.4.4	Il catalogo delle misure tecniche organizzative	»	98
3.5	<i>Data protection by design e data protection by default</i> : i concetti giuridici	»	108
3.6	Il risarcimento per violazione del Regolamento e violazione della privacy	»	113
3.7	Le sanzioni amministrative	»	116
3.7.1	Premessa	»	116
3.7.2	L’impianto sanzionatorio del Regolamento: caratteristiche	»	117
3.7.3	I criteri di ponderazione della sanzione amministrativa	»	117
3.7.4	Gli importi	»	119
3.7.5	Le tipologie di sanzioni previste	»	119
3.8	Le sanzioni penali nella normativa italiana	»	120
4.	L’Autorità Garante e la circolazione dei dati personali dentro e fuori l’Ue		
4.1	I meccanismi di comunicazione tra le Autorità di controllo	»	127
4.1.1	Premessa	»	127
4.1.2	La procedura di cooperazione (art. 60) e il meccanismo del c.d. “sportello unico”	»	128
4.1.3	Il Meccanismo di coerenza	»	133
4.1.4	La procedura di urgenza	»	135

4.2	Flussi transfrontalieri di dati personali e ruolo del Garante	»	135
4.2.1	Premessa	»	135
4.2.2	La nozione di trasferimento	»	136
4.2.3	L'adeguatezza e le garanzie adeguate	»	137
4.2.4	Alcune indicazioni di carattere pratico	»	139
4.3	Opportunità per le imprese: certificati e codici di condotta	»	142
4.3.1	Premessa	»	142
4.3.2	Codici di condotta	»	143
4.3.3	Meccanismi di certificazione	»	144
4.3.4	In attesa delle prassi.....	»	145
5.	Casi specifici di trattamento dei dati personali		
5.1	La protezione dei dati nella Pubblica Amministrazione.....	»	147
5.1.1	La PA come titolare <i>sui generis</i>	»	149
5.1.2	Legge applicabile e basi giuridiche.....	»	150
5.1.3	L'accesso civico e la protezione dei dati personali	»	154
5.2	Il trattamento di dati in ambito giudiziario penale.....	»	155
5.3	La protezione dei dati personali in sanità: qualche specificità e coordinamenti necessari.....	»	163
5.4	Protezione dei dati personali e <i>marketing</i> : l'impatto del Regolamento nelle attività aziendali <i>online</i>	»	167
5.5	Il trattamento dei dati in ambito lavorativo	»	169
5.6	Il trattamento dei dati a fini di ricerca	»	173
5.6.1	Premessa: big data e ricerca	»	173
5.6.2	Le conseguenze del passaggio dalla <i>privacy</i> alla protezione dei dati.....	»	173
5.6.3	Sulle basi giuridiche, il consenso, le sue alternative e deroghe	»	175
5.6.4	Le basi giuridiche per i dati particolari e ... le altre basi per la ricerca.....	»	175
5.6.5	Problematicità e soluzioni nel gioco tra regole ed eccezioni nel Regolamento e nelle norme nazionali.....	»	179
5.6.6	Trattamenti ulteriori e ricerca.....	»	181
5.6.7	Le specificazioni italiane per il riuso e i problemi transnazionali.....	»	182
5.6.8	Ambito e portata delle eccezioni di cui agli artt. 85 e 89: i limiti dell'attuazione nazionale.....	»	183
5.6.9	Il ruolo (non chiaro) delle regole deontologiche nazionali	»	186
5.6.10	Considerazioni di sintesi	»	186

5.7	Ai margini del GDPR: PMI, enti <i>no-profit</i> e titolari individuali alla prova dell'adeguamento alla nuova normativa.....	»	188
5.7.1	Introduzione.....	»	188
5.7.2	PMI, liberi professionisti e enti <i>no-profit</i> : come individuare gli adempimenti obbligatori	»	189
5.7.3	Gli obblighi di informazione ex art. 13-14 GDPR	»	190
5.7.4	Il registro dei trattamenti	»	193
5.7.5	La valutazione di impatto sulla protezione del dato e la nomina del DPO	»	196
6.	L'implementazione tecnologica ed organizzativa delle regole sul trattamento dei dati personali		
6.1	Tecnologie abilitanti per la sicurezza e privacy dei dati	»	199
6.1.1	Sicurezza informatica e <i>privacy</i>	»	201
6.1.2	<i>Privacy</i> e anonimizzazione	»	202
6.1.3	Sicurezza informatica e pragmaticità	»	202
6.2	Criticità per la privacy del cittadino nell'era dei Big Data.....	»	204
6.2.1	<i>Privacy, Big-Data Processing e Cloud Computing</i>	»	205
6.2.2	Conclusioni	»	206
6.3	L'impatto del GDPR sulle strategie ICT: il ruolo del DPO oltre la teoria 206		
6.3.1	Gestione della raccolta e classificazione del dato e modalità di elaborazione	»	209
6.3.2	Protezione del dato	»	210
6.3.3	Gestione dei diritti del cittadino.....	»	211
6.3.4	Verifica della conformità per servizi esternalizzati in <i>cloud</i>	»	213
6.3.5	Gestione degli incidenti	»	214
6.4	Integrità e disponibilità del dato: la continuità operativa IT	»	215
6.4.1	La continuità operativa	»	217
6.4.2	Le tecniche di protezione del dato.....	»	218
6.4.3	L'approccio moderno alla continuità operativa	»	221
6.4.4	<i>Disaster recovery</i>	»	222
	Appendice		
	Decreto legislativo 30 giugno 2003, n. 196 [Codice della privacy].....	»	223
	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016	»	269

Profilo autori

ANGELA D'ANGELO

Dottore di Ricerca in Diritto Privato, Avvocato presso il Foro di Pisa, Affiliata al Lider-Lab della Scuola Superiore Sant'Anna di Pisa.

DENISE AMRAM

Dottore di Ricerca in Diritto di Privato ed Avvocato del foro di Pisa, DPO.

GIOVANNI COMANDÉ

Professore Ordinario di Diritto Privato Comparato presso la Scuola Superiore Sant'Anna di Pisa dove dirige il Laboratorio Interdisciplinare Diritti e Regole, Avvocato del foro di Pisa e nello Stato di New York USA; fondatore di www.smartlex.eu.

TOMMASO CUCINOTTA

Professore Associato presso l'Istituto TeCIP della Scuola Superiore Sant'Anna di Pisa.

CLIZIA D'AGATA

Dottore di Ricerca in Diritto Privato, Funzionaria presso il Garante per la protezione dei dati personali.

GAIA FIORINELLI

Dottoranda di ricerca in Diritto Penale presso la Scuola Superiore Sant'Anna di Pisa.

MARIA GAGLIARDI

Professore Associato di Diritto Privato presso la Scuola Superiore Sant'Anna di Pisa.

ITALO LISI

Chief of Information Officer presso la Scuola Superiore Sant'Anna di Pisa.

GIANCLAUDIO MALGIERI

Dottorando presso *il Law, Science, Technology and Society (LSTS) Research Group* della Free University of Brussels (VUB), avvocato e docente in tema di protezione dei dati personali, Affiliato al Lider-Lab della Scuola Superiore Sant'Anna di Pisa.

ANNA MONREALE

Ricercatore di Informatica presso l'Università di Pisa.

MARIA BEATRICE PIERACCINI

Dottore di Ricerca in Diritto Pubblico dell'Economia, Avvocato presso il Foro di Lucca, Affiliata al Lider-Lab della Scuola Superiore Sant'Anna di Pisa, DPO.
