Caterina Tosatti

Privacy e Data Protection

Guida al Regolamento (UE) 2016/679 per imprese, professionisti, PA e Responsabili della Protezione Dati (DPO)

SECONDA EDIZIONE *aggiornata al*
DLgs del 10 agosto 2018, n. 101

dei
GIURIDICA

Caterina Tosatti, Avvocato presso il Foro di Roma, dopo la laurea magistrale in giurisprudenza presso l'Università di Bologna e l'abilitazione alla professione forense, ha frequentato il Master di management pubblico e preparazione alla S.S.P.A. presso il CEIDA in Roma. Ha inoltre collaborato con studi legali nella materia della Responsabilità degli Enti ai sensi del DLgs 231/2001, dove ha approfondito la materia della privacy. È divenuta inoltre Mediatore e Formatore ai sensi del DM 180/2010, acquisendo elevate capacità nel campo della negoziazione, problem solving e conflict management.

Via Cavour, 179/A - 00184 Roma
Tel. 06.441.63.71 (r.a.) Fax 06.440.33.07
e-mail dei@build.it
URL http://www.build.it

INDICE

Introduzione 07

1. GDPR: OGGETTO, FINALITÀ, AMBITO DI APPLICAZIONE 13
1.1. Origine del GDPR 13
1.2. L'oggetto e le finalità del GDPR 17
1.3. L'ambito di applicazione materiale e territoriale 20
1.3.1. L'ambito di applicazione materiale 20
1.3.2. L'ambito di applicazione territoriale 28
1.4. I 6 principi + 1 del trattamento 33
1.5. La "liceità" del trattamento: le basi giuridiche 37
1.5.1. Il Consenso secondo GDPR 42
1.5.2. L'interessato 'minore' e i servizi della società dell'informazione 52
1.6. 'Particolari' dati personali e dati relativi a condanne penali e reati 56
1.7. Trattamento che non richiede l'identificazione 63
GDPR in pillole 64
CHE FARE 67

2. L'INFORMATIVA PRIVACY E I 'NUOVI' DIRITTI DELL'INTERESSATO 69
2.1. L'informativa all'interessato 69
2.2. L'Informativa artt. 13 e 14 GDPR 73
2.2.1. L'Info Privacy ex art. 13 GDPR 74
2.2.2. L'Info Privacy ex art. 14 GDPR 84
2.3. Art. 15 GDPR: il diritto di accesso 86
2.4. Artt. 16 e 17 GDPR: diritti di rettifica e cancellazione (oblio) 88
2.5. Art. 18 e 19 GDPR: limitazione al trattamento e onere di notifica 93
2.6. Art. 20 GDPR: diritto alla 'portabilità' 97
2.7. Art. 21 GDPR: diritto di opposizione al trattamento 100
2.8. Art. 22 GDPR: processi decisionali automatizzati e profilazione 103
2.9. Art. 23 GDPR: limitazioni all'esercizio dei diritti dell'interessato 107
GDPR in pillole 110

3. LA *ACCOUNTABILITY* DEL TITOLARE E DEL RESPONSABILE DEL TRATTAMENTO 123
3.1. Il titolare del trattamento ed i suoi obblighi / oneri 123
3.1.1. La responsabilità del Titolare: misure adeguate, Codici di Condotta e Certificazione 126
3.1.2. La sicurezza dei dati e la Data Breach 133
3.2. Il Responsabile del trattamento ed i suoi obblighi / oneri 148
3.2.1. La 'responsabilità' del Responsabile: artt. 28 e 29 GDPR 149
3.2.2. La sicurezza dei dati e la Data Breach 153
3.3. I Registri delle attività di trattamento 155
3.4. La DPIA e la Consultazione Preventiva 157
3.5. Il DPO 168
GDPR in pillole 172
CHE FARE 179

4. TRASFERIMENTI DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI 181
CHE FARE 190

5. DPA, SANZIONI E RICORSI 191
5.1. Competenze, compiti e poteri delle DPAS: la *Leading* DPA e il *Board* 191
5.2. I mezzi di ricorso 'amministrativi' e giurisdizionali 197
5.2.1. Responsabilità e diritto al risarcimento 199
5.3. Le sanzioni amministrative: condizioni generali per infliggerle e misura 200

Bibliografia 205