

Giancarlo Butti,
Maria Roberta Perugini

GDPR La privacy nella pratica quotidiana

Tutte le domande a cui un DPO
deve sapere rispondere



FrancoAngeli

MANAGEMENT

TOOLS

Indice

Introduzione	pag.	13
Convenzioni utilizzate nel testo	»	14
1. Perimetro di applicazione e tutela	»	17
1. Quali sono le normative che regolamentano la protezione dei dati personali?	»	17
1.1. Normativa europea	»	17
1.1.1. Regolamenti e Direttive	»	17
1.2. Normativa italiana in ambito privacy	»	19
1.3. Normativa italiana che ha impatti in ambito privacy	»	19
1.4. Altre normative nazionali in ambito UE	»	19
1.5. Altre normative nazionali in ambito extra UE	»	20
1.6. Come gestire tutte queste normative?	»	20
2. Qual è l'ambito di applicazione del GDPR?	»	21
2.1. L'ambito di applicazione materiale	»	21
2.2. L'ambito di applicazione territoriale	»	23
3. Cosa è un dato personale?	»	24
3.1. Cosa si intende per "qualsiasi informazione"?	»	25
3.2. A chi si riferisce?	»	26
3.3. Cosa si intende per "identificati"?	»	27
3.4. Cosa si intende per "identificabili"?	»	27
3.5. Cosa non è dato personale?	»	28
4. Cosa è un dato particolare?	»	29
5. Chi sono i soggetti tutelati nel contesto della normativa privacy?	»	32
5.1. GDPR	»	32
5.2. D.lgs. 196/03	»	32
6. Chi e quali sono gli interessati?	»	33
6.1. Chi e quali sono le persone fisiche?	»	36
6.2. Cosa sono i diritti e le libertà delle persone fisiche?	»	38

2. Accountability, privacy by design e by default	pag.	41
1. Che cosa è l'accountability?	»	41
1.1. Come è possibile progettare, attuare e controllare la conformità del trattamento?	»	42
1.2. Come è possibile dimostrare la conformità?	»	43
1.3. Esiste un set minimo di documenti obbligatori?	»	44
1.4. Quali sono i collegamenti fra i vari adempimenti?	»	46
2. I Registri delle attività di trattamento sono obbligatori per tutti?	»	47
2.1. A cosa serve il Registro?	»	48
2.2. Da dove si parte per la corretta compilazione dei Registri?	»	49
2.3. Che strumenti posso utilizzare?	»	50
2.4. Qual è il livello di granularità con cui effettuare la mappatura?	»	51
2.5. Esistono linee guida sull'argomento?	»	52
3. La "privacy by design" è una novità del GDPR?	»	53
3.1. Era effettivamente necessario formalizzare tale richiesta in una normativa?	»	54
3.2. Cosa si intende per privacy by default (protezione per impostazione predefinita)?	»	54
3. Ruoli di trattamento	»	57
1. Come si valuta il ruolo da attribuire?	»	57
1.1. Siamo consapevoli del nostro contesto di trattamento?	»	57
1.2. Quali sono gli impatti del ruolo di un soggetto sul suo modello privacy?	»	59
1.3. È possibile rivestire più ruoli contemporaneamente nei confronti di un altro soggetto?	»	59
2. Cosa si intende per Responsabile?	»	60
2.1. Esiste ancora il Responsabile interno?	»	61
2.2. Quali sono le conseguenze di una designazione a Responsabile sulla propria catena di designazioni?	»	62
2.3. È possibile una designazione incrociata?	»	62
3. Che ruolo hanno le persone fisiche che operano sotto le direttive del Titolare o del Responsabile?	»	62
3.1. Quali sono i vincoli per l'autorizzazione al trattamento?	»	64
4. Come si formalizzano i ruoli?	»	65
5. Esistono modelli ufficiali per l'attribuzione dei ruoli?	»	67
6. Esistono ancora gli amministratori di sistema?	»	67
4. Sicurezza	»	71
1. Misure di sicurezza	»	71
1.1. Esistono misure di sicurezza obbligatorie?	»	71

1.2. Il Titolare è obbligato ad esempio a cifrare i dati o ad utilizzare la pseudonimizzazione?	pag.	73
1.3. Le misure minime sono ancora obbligatorie?	»	74
1.4. Come si determinano le misure di sicurezza adeguate?	»	74
1.5. Esistono cataloghi di misure di sicurezza cui fare riferimento?	»	75
1.6. Esistono cataloghi ufficiali di misure di sicurezza cui fare riferimento?	»	75
1.7. Esistono buone pratiche di riferimento?	»	76
2. Ma l'analisi dei rischi è la DPIA?	»	76
2.1. Come si svolge e cosa comprende un'analisi dei rischi?	»	77
2.2. Esistono metodologie ufficiali per lo svolgimento dell'analisi dei rischi?	»	79
2.3. Esistono strumenti ufficiali per l'analisi dei rischi?	»	79
2.4. Perché è opportuno utilizzare metodologie ufficiali per svolgere un'analisi dei rischi?	»	80
2.5. Qual è il livello di granularità con cui svolgere un'analisi dei rischi ai sensi dell'art. 32?	»	80
3. Che differenza c'è fra analisi dei rischi e DPIA?	»	81
3.1. Quando deve essere eseguita una DPIA?	»	82
3.2. Si può svolgere comunque una DPIA anche se non è obbligatoria?	»	83
3.3. Come si svolge e cosa comprende una DPIA?	»	83
3.4. Esistono metodologie ufficiali per lo svolgimento di una DPIA?	»	84
3.5. È possibile utilizzare metodologie non ufficiali per svolgere una DPIA?	»	84
3.6. Qual è il livello di granularità con cui svolgere una DPIA?	»	85
5. Gestione dei diritti	»	87
1. Chi può esercitare i diritti?	»	87
1.1. Quali sono i nuovi diritti e che cosa comportano in termini tecnici ed organizzativi?	»	87
2. Che differenza c'è fra diritto di accesso e portabilità?	»	89
2.1. Quali sono i dati che devono essere forniti all'interessato in base al diritto di accesso?	»	90
2.2. Come devono essere forniti i dati?	»	90
2.3. C'è qualche vincolo nella comunicazione dei dati all'interessato?	»	91
2.4. Quando è esercitabile il diritto alla portabilità?	»	92
2.5. Quali sono i dati che devono essere forniti all'interessato in base al diritto di portabilità?	»	92
2.6. Come fa il Titolare a identificare l'interessato prima di rispondere a una sua richiesta?	»	93

6. Principi	pag.	95
1. Come vengono determinati i tempi di conservazione?	»	95
1.1. Come si stabiliscono i tempi di conservazione determinati da vincoli esterni?	»	95
1.2. Da quando inizia il conteggio del periodo di conservazione?	»	97
1.3. Come si stabiliscono i tempi di conservazione per fini autodeterminati?	»	97
1.4. Come si rappresentano i tempi di conservazione all'interno delle informative o nei Registri delle attività di trattamento?	»	98
1.5. Si possono estendere i tempi di conservazione originari?	»	98
1.6. Cosa succede se i dati devono essere utilizzati nell'ambito di un contenzioso oltre i termini di conservazione previsti?	»	99
1.7. È obbligatorio conservare i dati oltre i termini previsti per potere rispondere a potenziali richieste degli organi inquirenti?	»	99
1.8. Dove vanno indicati i tempi di conservazione?	»	100
1.9. Per quanto tempo si possono conservare i dati nella posta elettronica?	»	100
1.10. Al termine del tempo di conservazione i dati vanno necessariamente cancellati?	»	100
1.11. Esistono buone pratiche in merito alla cancellazione?	»	101
2. Quali aspetti è necessario considerare al fine di una corretta mappatura dei dati?	»	102
2.1. Devono essere mappati tutti i dati?	»	103
3. Cosa vuol dire che il dato deve essere esatto?	»	103
3.1. È possibile definire indicatori sulla qualità dei dati?	»	105
3.2. Dove è necessario intervenire per garantire la qualità del dato?	»	106
3.3. Quali sono gli interventi che è possibile mettere in atto per migliorare la qualità dei dati; quali i controlli?	»	106
3.4. Esistono standard di riferimento?	»	108
7. Certificazioni	»	109
1. In cosa consistono le certificazioni previste dal GDPR?	»	109
1.1. Chi può ottenere la certificazione?	»	109
1.2. Cosa si può certificare?	»	109
1.3. Chi rilascia tali certificazioni?	»	110
1.4. Quanto dura la certificazione?	»	110
1.5. Chi definisce i criteri di certificazione?	»	111
1.6. È già possibile certificarsi?	»	111

2. Che ruolo hanno in questo contesto le certificazioni ISO?	pag. 111
2.1. Ma tutte le norme ISO sono certificabili?	» 112
2.2. La conformità alla certificazione ISO 27001 è sufficiente a garantire la piena conformità alle prescrizioni del GDPR?	» 112
3. In cosa consistono le certificazioni pubblicizzate da diversi enti per diversi ruoli privacy, compreso quello del DPO?	» 115
3.1. Chi rilascia tali certificazioni?	» 115
3.2. Esistono albi professionali?	» 116
3.3. Esistono certificazioni ufficiali?	» 116
3.4. Esistono altre certificazioni?	» 116
8. Codici di condotta	» 117
1. Cosa sono i Codici di condotta?	» 117
1.1. Come si realizza un Codice di condotta?	» 118
1.2. Esistono esempi di Codici di condotta?	» 118
1.3. Chi effettua i controlli in merito all'osservanza di un Codice di condotta?	» 120
9. Verifiche	» 121
1. Perché svolgere verifiche in ambito privacy?	» 121
1.1. A che tipo di sanzioni è esposta l'azienda?	» 121
1.2. Per quale motivo parliamo di verifiche e non di audit in senso stretto?	» 122
1.3. Quali sono i tipi di verifiche da svolgere in ambito privacy?	» 123
1.4. Perché l'audit privacy sul GDPR è diverso rispetto a quanto effettuato in precedenza?	» 124
1.5. Quali sono i rischi delle verifiche in ambito privacy?	» 124
2. Quali sono gli strumenti più idonei per lo svolgimento delle verifiche?	» 126
2.1. Ci sono degli strumenti ufficiali?	» 126
3. Come si deve procedere per una verifica effettiva?	» 126
3.1. Quali sono gli elementi che caratterizzano un audit negli ambiti formalizzati?	» 128
3.2. Quali sono gli elementi che caratterizzano un audit negli ambiti non formalizzati?	» 129
4. Come è possibile valutare la conformità?	» 130
5. Che differenza c'è fra audit e consulenza?	» 131
5.1. Chi può effettuare verifiche in ambito privacy?	» 132
5.2. Chi non può effettuare verifiche in ambito privacy?	» 132
5.3. È possibile verificare l'operato del DPO?	» 132
5.4. Che relazioni vi sono fra le varie strutture di controllo in merito al rispetto della normativa privacy?	» 133

10. La responsabilità del DPO	pag. 135
1. Quali sono le responsabilità del DPO?	» 135
1.1. Il DPO risponde per la non conformità dei trattamenti dell'ente designante e per i trattamenti attuati nell'esercizio delle proprie funzioni?	» 135
1.2. Il DPO può incorrere in responsabilità per inadempimento?	» 136
1.3. Conflitto di interessi: quali sono le conseguenze in termini di responsabilità per il DPO?	» 138
11. Esempi applicativi	» 141
1. Esempio 1 – Implementare l'attività di smartworking	» 141
1.1. Lo scenario	» 141
1.2. Le soluzioni tecniche e organizzative	» 142
1.3. Gli adempimenti privacy	» 144
1.4. La valutazione dei rischi	» 145
1.5. Gli scenari di rischio	» 146
1.6. Le idonee misure tecniche e organizzative	» 149
2. Esempio 2 – Come definire correttamente il ruolo di trattamento e attribuire le relative responsabilità in termini di adempimenti? Il caso delle finalità di marketing	» 151
Bibliografia	» 155

Introduzione

L'idea di questa pubblicazione nasce dall'esperienza maturata non solo nel corso dell'attività professionale ma anche in occasione dei numerosi corsi e master che ci hanno visti come docenti in questi anni.

Molto spesso, nonostante il livello di preparazione degli allievi fosse alto ed il loro ruolo rilevante (molti DPO e consulenti), riscontravamo aree grigie in merito a elementi basilari relativi alla conoscenza della normativa, foriere di rilevanti conseguenze.

Una non corretta individuazione di quali siano i dati personali trattati dalla propria organizzazione o delle categorie di interessati può fare sì che il perimetro di applicazione di tutte le misure messe in atto per il rispetto della normativa privacy sia errato, escludendo dalla tutela fasce più o meno rilevanti di persone fisiche o di dati personali.

Le conseguenze sono il rischio di sanzioni o di risarcimento danni ai sensi dell'art. 82 del GDPR, oltre agli effetti negativi indiretti connessi alla perdita d'immagine dell'organizzazione Titolare.

A questo esempio se ne possono aggiungere molti altri, derivanti da un approccio troppo spesso meccanicistico e scolastico nei confronti di una normativa eccezionalmente complessa, articolata e ricca di interazioni sia interne (intendendo con tale termine il legame, spesso non evidente, fra i vari adempimenti normativi) sia esterne.

A ciò spesso contribuisce la scarsa conoscenza della normativa, appresa più per "sentito dire", tramite corsi e pubblicazioni, piuttosto che dalla sua lettura diretta, nonché una analisi troppo superficiale.

Ecco quindi che credenze diffuse si diffondono e mistificano la norma.

Molti confondono la DPIA con l'analisi dei rischi, o scambiano i diritti e libertà delle persone fisiche (come recita la normativa) con quelli dei soli interessati.

Da qui la necessità di fare chiarezza e il motivo per cui, in luogo di semplici interpretazioni, è importante ripartire dal testo effettivo della normativa, troppo spesso ignorato.

Il libro vuole essere uno strumento realmente operativo, ma anche rigoroso nei contenuti. Per tale motivo, in luogo di una serie di modelli e modulistica autoprodotta sono riportate nelle appendici (disponibili on line) i riferimenti a modulistica e strumenti “ufficiali”, in quanto proposti da Autorità Garanti.

Infine, pur volendo essere il più possibile oggettivo, il testo riporta ovviamente le opinioni degli autori¹ e come tale deve essere considerato.

Lo spazio necessariamente limitato ci ha costretto a selezionare alcuni argomenti e temi tralasciandone altri, e il taglio strettamente operativo non ci ha consentito di sviluppare verticalmente alcune questioni di cui abbiamo fornito direttamente le conclusioni: ove possibile abbiamo suggerito in nota fonti utili per approfondire.

Segnaliamo infine che nel nostro blog professionale www.mrperugini.it, oltre a studi e documenti utili, è presente una sezione dedicata a questo libro in cui pubblicheremo note e articoli di approfondimento e aggiornamento dei temi qui trattati e dove affronteremo altre problematiche di interesse per i DPO.

In particolare, contestualmente alla pubblicazione del testo saranno disponibili una serie di Appendici.

Per la realizzazione del testo sono stati utilizzati contributi che negli anni sono stati pubblicati in particolare sul blog collettivo blog.europrivacy.info e sulle riviste online Cybersecurity360 (cybersecurity360.it), Cybersecurity Trends (www.cybertrends.it/rivista/), Toolnews (itware.com).

Al riguardo un ringraziamento va ad Alessandro Longo, Alessandro Giachino, Elena Agresti.

Alcuni spunti derivano inoltre dalla nostra precedente pubblicazione del 2019 per FrancoAngeli “Audit e GDPR - Manuale per le attività di verifica e sorveglianza del titolare e del DPO (Data Protection Officer)”.

Convenzioni utilizzate nel testo

All’interno di questo documento si utilizzeranno le seguenti convenzioni. Il termine “soluzioni ufficiali” indica che tali soluzioni sono realizzate:

- da autorità garanti degli Stati membri;
- dall’autorità garante europea – edps.europa.eu;
- dal Comitato europeo per la protezione dei dati (ex WP29) – edpb.europa.eu/edpb_it;
- da ENISA – www.enisa.europa.eu/;

il termine “normativa” può comprendere anche le “soluzioni ufficiali”; il termine “soluzioni autorevoli” indica che sono realizzate da enti di normazione, quali:

1. Opinioni che derivano da oltre 20 anni di “pratica” nel campo della protezione dei dati personali.

- ISO – www.iso.gov;
- NIST – www.nist.gov.

Si citeranno inoltre:

- Autorità Garante (Autorità Garante per la protezione dei dati personali italiana) – www.garanteprivacy.it/;
- CNIL – Commission Nationale de l’Informatique et des Libertés (Autorità di controllo francese) – www.cnil.fr;
- AEPD (Autorità di controllo spagnola) – www.aepd.es;
- ICO Information Commissioner’s Office (Autorità di controllo inglese) – ico.org.uk;
- OECD (Organisation for Economic Co-operation and Development) – www.oecd.org/.

I termini “titolare” e “responsabile”, quando indicano i relativi ruoli previsti dagli artt. 24 e 28 del GDPR saranno scritti, a soli fini identificativi, come Titolare e Responsabile.

I termini “azienda”, “organizzazione”, “ente” vengono spesso utilizzati per indicare genericamente un ente che effettua un trattamento di dati personali.

Il termine “privacy” viene utilizzato generalmente per intendere la complessiva normativa applicabile in materia di protezione dei dati personali.