Giancarlo Butti - Alberto Piamonte

GDPR: NUOVA PRIVACY LA CONFORMITÀ SU MISURA

Prefazione a cura di Maria Roberta Perugini

Come sviluppare modelli per:

- Rispettare le regole
- Ottimizzare i costi
- Riutilizzare gli investimenti effettuati per il D.Lgs 196/2003
- Cogliere le opportunità di sinergie e sviluppo organizzativo

ITER®

Aggiornamenti su www.iter.it/gdpr

GDPR NUOVA PRIVACY

LA CONFORMITÀ SU MISURA

di Giancarlo Butti e Alberto Piamonte

GDPR NUOVA PRIVACY

LA CONFORMITÀ SU MISURA

di Giancarlo Butti e Alberto Piamonte

EDITORE

ITER Srl – Milano

Via A. Sacchini, 20

20131 Milano (MI)

www.iter.it

ISBN 9788890341915

STAMPA

Digital book s.r.l.
Via Karl Marx, 9
06012 Cerbara - Città di Castello (PG)

MATERIALE DI SUPPORTO

Il materiale di supporto a questo testo è disponibile sul sito dell'Editore.

Prima edizione

Finito di stampare nel mese di gennaio 2017

A mia moglie.
Ai 4 pargoletti che vivono con noi.
(Billy, River, Lord, Chery)
Alle centinaia a cui abbiamo trovato
una casa e una famiglia.
Alle migliaia ai quali vogliamo trovarle.
Giancarlo

Ringraziamenti
Grazie ad Alberto, Domenico ed Annalisa
che hanno permesso la realizzazione
di quest'opera ed a Roberta
che ne ha curato la Prefazione.
Giancarlo

A mia moglie Lia, per la pazienza.
Alberto

Ringraziamenti
Grazie a Giancarlo
per l'opportunità che mi ha offerto,
a Laura e Piero per i preziosi consigli.
Alberto

Giancarlo Butti *(giancarlo.butti@promo.it)*

(LA BS 7799), (LA ISO IEC 27001), CRISC, ISM, DPO, CBCI, AMBCI

Master di II livello in Gestione aziendale e Sviluppo Organizzativo (MIP - Politecnico di Milano).

Si occupa di ICT, organizzazione e normativa dai primi anni 80:

- analista di organizzazione, project manager, security manager ed auditor presso gruppi bancari
- consulente in ambito documentale, sicurezza, privacy… presso aziende di diversi settori e dimensioni.

Come divulgatore ha all'attivo:

- oltre 700 articoli su 20 diverse testate tradizionali e 7 on line
- 20 fra libri e white paper, alcuni dei quali utilizzati come testi universitari
- 6 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT sulla sicurezza ICT in Italia
- membro della faculty di ABI Formazione e docente presso altre istituzioni
- relatore presso eventi di ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF…

Socio e proboviro di AIEA/ISACA (www.aiea.it – Associazione Italiana Information Systems Auditors) e socio del CLUSIT (www.clusit.it – Associazione Italiana per la Sicurezza Informatica).

Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity e Rischio informatico, di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su privacy, frodi, eidas, sicurezza dei pagamenti, di UNINFO sui profili professionali privacy…

Fra i coordinatori di www.europrivacy.info.

Alberto Piamonte *(alberto.piamonte@alice.it)*

Alberto Piamonte, laureato nell'Università di Padova in Ingegneria Elettronica, fa attualmente parte del KeyMap Team, un gruppo di Consulenti ed Aziende che si occupa dello sviluppo di strumenti automatizzati e metodologie per attività di audit, l'analisi e gestione dei rischi, la certificazione conformità e la realizzazione di efficaci ed efficienti sistemi di controllo e di governo.

Oltre che svolgere in prima persona attività di consulenza si occupa attivamente dei problemi relativi al governo dei sistemi IT tenendo frequenti corsi e seminari su metodologie quali COBIT, ITIL e ISO27001 ed alla sensibilizzazione e diffusione delle relative tematiche, è stato Consigliere AIEA con il ruolo di Research Director.

Inizia la sua carriera come ricercatore IBM con permanenza più che decennale nei laboratori di ricerca e sviluppo (USA, Germania, Svezia ed Italia) occupandosi principalmente di comunicazioni (SNA) e relativi problemi di sicurezza.

Successivamente, come Direttore Responsabile del Marketing Olivetti per le Pubbliche Amministrazioni, è stato coinvolti nella gestione e realizzazione di grandi progetti**.**

Più recentemente come Direttore Software Europa di Amdahl Corporation si è occupato delle problematiche di gestione e sicurezza di grandi reti di utenti.

Socio di ISACA – Roma, COBIT5 Trainer, Assessor ed Implementor.

Εὕρηκα

Archimede

INDICE

GUIDA ALLA LETTURA DEL TESTO

PREFAZIONE

Sono passati ormai vent'anni dall'entrata in vigore in Italia della prima normativa a tutela dei dati personali, e da allora sia la complessità della regolamentazione sia la consapevolezza della collettività sui relativi temi è molto cresciuta, andando di pari passo con il vorticoso progresso tecnologico.

Oggi parliamo correntemente di "diritto alla protezione dei dati personali", ma molto spesso senza soffermarci sul reale contenuto di questo concetto.

Per acquisire una piena consapevolezza del suo significato è importante considerare che la codifica legislativa e regolamentare di un diritto è un processo che traduce sul piano dell'affermazione giuridica un'esigenza concreta manifestata dalla collettività, che scaturisce dal contesto socio economico e politico.

L'evoluzione tecnologica "in corsa" è diventata l'asse portante dello sviluppo sociale ed economico su un piano globale da quando all'informatizzazione dei dati – cominciata negli anni Settanta del '900 – alla metà degli anni Novanta si è aggiunta la loro circolazione su reti telematiche in un contesto (il *world wide web*) ove essi sono memorizzati e diffusi in forma frammentata e priva di qualsiasi organizzazione, decontestualizzati.

In tale cornice, la raccolta, l'elaborazione e lo scambio di dati personali sono diventati attività funzionali alla gestione ordinaria dell'attività di qualsiasi impresa, le occasioni e le finalità di trattamento si sono moltiplicate esponenzialmente, la crescita di servizi sempre più mirati necessita di disporre di informazioni sempre più analitiche: la disponibilità di dati personali ha assunto un rilevante valore economico, l'affermazione di nuove tecnologie (*cloud computing*, tecniche biometriche, uso delle tecnologie delle radiofrequenze (Rfid) per la creazione di oggetti "intelligenti", trattamento di dati genetici, geolocalizzazione, sviluppo dell'*e-government*) ha trasformato le relazioni sociali e dato incentivo alla creazione di nuovi modelli di utilizzo delle informazioni che inducono sempre maggiori rischi di perdita del controllo sui propri dati.

Di conseguenza, la richiesta sociale di protezione e di controllo sulle informazioni personali degli individui è altissima.

È in quest'ottica che dobbiamo leggere il Regolamento, le cui norme riconoscono un nuovo, autonomo, diritto fondamentale della persona umana: quello alla "protezione dei dati personali".

Questo diritto è la risposta al moderno atteggiarsi dell'esigenza dell'individuo di protezione delle informazioni che lo riguardano: come traspare dal complesso della normativa, il potere che il Regolamento attribuisce all'interessato supera la valenza tipicamente difensiva del tradizionale diritto alla riservatezza – inteso quale puro rispetto della vita privata della persona – per diventare un vero e proprio potere di disposizione, di gestione dei proprî dati, sostenuto dallo strumento costituito dal consenso informato e fondato sull'affermazione della prevalenza dei valori fondamentali per l'autonomia della persona: la dignità e l'uguaglianza in primo luogo.

È a ragione della dinamica descritta che la protezione dei dati personali oggi è uno dei temi guida nella regolamentazione dei processi di creazione del mercato unico digitale. La Commissione Europea sta operando per abbattere le barriere regolamentari fino ad instaurare un unico mercato digitale europeo al posto dei ventotto mercati nazionali ora esistenti: è stato valutato che ciò porterebbe grandi benefici all'economia europea e la creazione di centinaia di migliaia di nuovi posti di lavoro; ma per raggiungere questo risultato è necessario rafforzare la fiducia nei servizi digitali e nella relativa sicurezza, in particolare per quanto riguarda il trattamento dei dati personali.

Occorrono dunque norme non più limitate ai singoli Stati, per quanto uniformi, ma globali, e che siano capaci di lungimiranza, in grado di adattarsi al rapido mutamento delle tecnologie e delle strategie commerciali, idonee a rispondere all'esigenza di agevolare i sempre più complessi flussi di dati – che sono portatori di benefici in termini di sviluppo economico e sociale – ed a garantire nel contempo un alto livello di protezione ai dati personali: regole, insomma, in grado di garantire lo sviluppo sostenibile delle dinamiche tecnologiche.

In quest'ottica il Regolamento UE, richiamandosi all'art. 8 della Carta dei diritti fondamentali dell'Unione Europea, proclama il diritto della persona umana alla protezione dei dati personali quale *"diritto fondamentale"*, precisando che va *"considerato alla luce della sua funzione sociale"* e bilanciato con tutti gli altri diritti di analoga natura riconosciuti dalle norme europee (tra cui la libertà di espressione e di informazione e la libertà d'impresa, ma anche la dignità umana, libertà e uguaglianza, proclamati solennemente in apertura dalla Carta dei diritti fondamentali dell'Unione Europea), sulla base del criterio di proporzionalità.

Ne è conseguenza l'organizzazione di un sistema che, riconoscendo nella società dell'informazione la centralità del dato personale in quanto oggetto di trattamento, fornisce all'interessato gli strumenti per gestirne tanto il valore quale componente del patrimonio informativo circolante quanto il tradizionale valore collegato alla sfera intima, quest'ultimo rivalutato nell'ottica della tutela della proiezione sociale dell'interessato, anche *on line*.

Questa struttura di base, facendo riferimento a dinamiche d'interazione tra diritti fondamentali, nella sua applicazione concreta non sconta più i tradizionali limiti di conformità a norme testuali a perenne rischio di obsolescenza, e costituisce dunque la griglia dinamica e flessibile, capace di adattarsi ai mutamenti tecnologici senza perdere efficacia, in coerenza con la quale sviluppare regole di dettaglio: attività cui concorrono l'iniziativa delle Autorità di controllo nazionali (ad esempio, emettendo autorizzazioni nei casi loro demandati), degli organismi comunitari (la Commissione, il Comitato Europeo per la protezione dei dati) e, ricorrendo specifiche circostanze, degli Stati membri e perfino degli accordi collettivi e di quelli "aziendali".

Il risultato è l'istituzione nella UE di un sistema di regole di trattamento oggettive ed uniformi, che declinano (e, ove necessario, consentono di declinare a livello locale) in norme di principio e di dettaglio le dinamiche di intersezione tra i valori - guida costituiti dai diritti fondamentali della persona: il meccanismo così individuato è volto ad assicurare ex ante il mantenimento costante nel tempo dell'"adeguatezza" della protezione dei dati personali, in sintonia – invece che in contrapposizione – con il progresso tecnologico.

Sull'armatura costituita dal bilanciamento delle libertà fondamentali, il Regolamento tesse dunque una rete di principi generali e definizioni di riferimento, alcuni già contenuti nelle normative uniformi che lo precedono (liceità, trasparenza, pertinenza e non eccedenza del trattamento, esattezza dei dati trattati) e altri codificati in linea generale per la prima volta (trasparenza e semplificazione, effettività della tutela, *data protection by design e by default*) seppure derivati dalla pratica applicativa e interpretativa di questi anni tanto della Corte di Giustizia e della Corte Europea dei Diritti dell'Uomo quanto delle Autorità preposte al controllo e della Commissione, tutte queste ultime operanti in seno all'Article 29 Working Party (organismo indipendente con funzioni consultive e di indirizzo composto da rappresentanti del Garante Europeo, delle Autorità indipendenti nazionali e della Commissione).

In questo contesto, vengono approntati gli strumenti concreti per il bilanciamento tra sviluppo economico e protezione dei dati personali: da un lato, il rafforzamento del consenso informato – a servizio del controllo *ex ante* sui proprî dati da parte dell'interessato – accompagnato, a presidio del controllo *ex post*, dall'ulteriore sviluppo dei rimedi – sia giurisdizionali sia esercitabili presso il titolare – per la tutela dell'interessato il cui diritto alla protezione dei dati sia violato.

Dall'altro lato, l'affermazione di quello che è stato chiamato "principio di responsabilità" o, in inglese, "accountability".

Il principio di responsabilità non è una novità nel contesto normativo europeo e internazionale: il suo espresso riconoscimento è già effettuato nelle linee guida per la protezione della vita privata dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) adottate nel 1980, che enunciano: *"Il responsabile del trattamento dei dati dovrebbe essere responsabile del rispetto delle misure che rendono effettivi i principi indicati sopra"*.

Tale principio è stato anche inserito esplicitamente tra gli standard internazionali di Madrid, elaborati dalla Conferenza internazionale sulla protezione dei dati e la *privacy* [1].

È inoltre accolto nel più recente progetto di norma ISO 29100 che stabilisce un quadro per la *privacy* riferito a un ambiente ICT, ed è uno dei principali concetti del quadro giuridico sulla *privacy* sviluppato dall'APEC e delle sue norme sulla *privacy* transfrontaliera.

Il principio di responsabilità è infine naturalmente già presente anche nella Direttiva 95/46/CE, ma espresso in disposizioni specifiche, e come tale è ripreso dal Codice Privacy italiano: un esempio è l'art. 31 di tale Codice, che rimette alla responsabilità del titolare l'adozione di misure di sicurezza "idonee".

Ma da tempo le istituzioni europee, e in particolare l'Art. 29 Working Party [2], hanno rilevato come nel sistema nato dalla direttiva 95/46/CE gli obblighi e principi fondamentali in materia di protezione dei dati personali abbiano trovato insufficiente applicazione a livello di misure e pratiche sostanziali, con i conseguenti rischi e inefficienze in rapporto alla protezione dei dati personali.

A fronte di questa constatazione, la risposta legislativa all'esigenza di traduzione degli obblighi fondamentali in meccanismi efficaci, atti a fornire una protezione reale, è stata l'introduzione – con il Regolamento – di una norma generale di responsabilità [3] che, per la sua architettura giuridica, persegue lo scopo di rafforzare il ruolo del titolare in rapporto al trattamento, definendone una responsabilità sì aumentata, ma nello stesso tempo caratterizzata da contenuti più concreti e chiari oltre che adattabili – nella loro traduzione pratica – in funzione di scelte effettuate dal titolare sulla base della propria autonoma determinazione dei rischi connessi al trattamento.

Già da un primo esame dell'architettura giuridica del principio di responsabilità appare evidente come il Regolamento strutturi un sistema di regole che non esprime solo obblighi, ma soprattutto fornisce un quadro di riferimento composto da obiettivi (effettuare il trattamento nel rispetto dei diritti e libertà delle persone fisiche e dunque nell'ottica della prevenzione adeguata ed efficace del rischio insito nel trattamento) e dagli strumenti per raggiungerli, rimettendo però al titolare stesso di modularne l'utilizzo assumendosi la responsabilità di individuare in fase tanto di progettazione quanto di esecuzione l'esistenza di rischi di violazione dei diritti degli interessati, di valutarne natura, probabilità e gravità, derivandone autonome decisioni e facendosi carico delle relative conseguenze [4], nonché di essere in grado di dimostrare che il trattamento è conforme alle norme.

---

[1] *La persona responsabile deve:*
"a. adottare tutte le misure necessarie per rispettare i principi e gli obblighi istituiti dal presente documento e dalla normativa nazionale vigente e
b. predisporre i meccanismi interni necessari per dimostrare tale conformità sia agli interessati sia alle autorità di controllo nell'esercizio dei loro poteri, come stabilito alla sezione 23".

[2] *Cfr. Art. 29WP, Parere 3/2010 sul principio di responsabilità, adottato il 13 luglio 2010.*

[3] *GDPR, art. 24: "1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. (...)".*

[4] *Numerosi ed immediati esempi si trovano nelle norme della Sezione 2, sulla sicurezza dei dati: l'applicazione "se del caso" delle misure elencate all'art. 32 comma 1, la scelta di notificare o meno i data breach a seconda della probabilità che essi comportino un rischio per i diritti degli interessati, la valutazione dell'"elevatezza" del rischio per i medesimi diritti che condiziona l'obbligo di notifica all'interessato, ecc.).*
Un esempio significativo della responsabilità descritta è costituito dalla previsione della rimessione al titolare della valutazione della possibilità di attenuazione del rischio evidenziato dalla valutazione d'impatto: essa infatti comporta la conseguenza di dovere decidere se coinvolgere l'Autorità di controllo in una consultazione preventiva – e rischiare di sottoporsi agli invasivi poteri di indagine dell'Autorità stessa (artt. 35 e 58) – o rischiare di vedersi contestare successivamente la violazione dei diritti degli interessati ad opera di una violazione di dati personali il cui rischio non poteva essere attenuato.

Il Regolamento ha dunque procedimentalizzato, sviluppato ed esteso a tutti i soggetti che operano il trattamento (titolari e responsabili) il principio di assunzione di responsabilità, e ciò tanto sotto il profilo della progettazione, attuazione e controllo del trattamento quanto sotto quello della responsabilità risarcitoria dei danni derivanti all'interessato dalla violazione dei suoi diritti perpetrata dal titolare o dal responsabile.

Coerente con l'esigenza di sollecitazione dei soggetti del trattamento all'assunzione di responsabilità attiva è anche la scelta di rafforzare l'impianto sanzionatorio per la violazione del Regolamento, commisurando l'entità della sanzione a circostanze soggettive concernenti il trattamento, nell'ottica di applicare sanzioni che siano *"effettive, proporzionate e dissuasive".* Questo obiettivo è perseguito sia mediante la fissazione di sanzioni amministrative pecuniarie articolate ed economicamente assai gravose (fino a 20 milioni di euro e al 4% del fatturato annuo di gruppo) sia mediante la chiara affermazione della esistenza ed autonomia della responsabilità anche risarcitoria dei varî soggetti attivi del trattamento (titolare, contitolari, responsabile, titolare apparente) per le violazioni degli obblighi legati al loro ruolo in tale contesto.

Insomma, l'impressione è che proprio nella nuova concezione di responsabilità si rifletta quel necessario bilanciamento tra diritti fondamentali volto a supportare il mantenimento dell'equilibrio tra l'espansione economica trainata dallo sviluppo tecnologico e le garanzie di salvaguardia dei diritti delle persone: si può dire che il Regolamento demanda al titolare del trattamento il quotidiano bilanciamento tra il diritto dell'interessato alla protezione dei dati personali ed i propri diritti, che si tratti di libertà d'impresa piuttosto che di espressione e di critica.

Entrando dunque un po' più nello specifico delle articolazioni del principio di *accountability*, si può verificare che lo schema giuridico approntato dal Regolamento a servizio dell'attuazione della responsabilità generale attiva del titolare è composto da un primo livello di meccanismi obbligatori praticamente per tutti: la progettazione ed attuazione di misure o procedure efficaci e adeguate e la conservazione delle relative prove; a questo si aggiunge un secondo livello, comprendente strumenti eccedenti le norme minime, adottabili su base volontaria, quali certificazione, sigilli, adozione di codici di condotta.

Risulta chiaro da questo contesto che a carico del titolare del trattamento sorge l'onere di rivalutare integralmente la propria organizzazione aziendale nell'ottica di una ridefinizione dei trattamenti secondo criteri di necessità, proporzionalità e minimizzazione dell'uso di dati personali, *accountability, privacy by design e by default* e della costruzione di un sistema articolato, complesso e dinamico che sia in grado anche di dare evidenza del rispetto della normativa.

Tutto ciò richiede da un lato l'adozione di strumenti per una completa mappatura dei trattamenti effettuati e di quelli progettati, per effettuare l'analisi dei rischi da essi indotti sulla protezione dei dati, valutandone natura, probabilità e gravità ed individuando e attuando tutte le misure per attenuare il rischio (tecniche, organizzative, contrattuali); dall'altro lato, per essere in grado di dimostrare che il trattamento è effettuato conformemente alla normativa, il titolare dovrà formalizzare per iscritto *policy* e procedure, nonché disporre verifiche in ordine al loro rispetto, fornendo evidenze oggettive della relativa effettuazione,.

Preliminarmente a tutto ciò è necessario che i titolari del trattamento avviino quanto prima attività preparatorie in termini di valutazione dell'impatto del Regolamento sulla propria operatività, e dunque a supporto dello sviluppo di un piano di implementazione e di una approfondita valutazione delle risorse da stanziare per un progetto certamente assai impegnativo ma ormai inevitabile e urgente: considerata la portata innovativa della riforma e la mole di lavoro necessaria per affrontarla adeguatamente, il termine del 25 maggio 2018, data in cui il Regolamento (che in ogni caso è già vigente) diventerà efficace, è dietro l'angolo.

In quest'ottica, il libro "GDPR NUOVA PRIVACY - LA CONFORMITÀ SU MISURA" è ottimo per tempestività, completezza, approfondimento e chiarezza.

Già nel titolo il riferimento alla conformità "su misura" esemplifica efficacemente l'effetto fondamentale del sistema giuridico delineato, che è quello di spingere il titolare verso la costruzione del proprio personale percorso di conformità del trattamento alle norme: conformità che – come si è ricordato sopra – coincide in concreto con una prevenzione adeguata, efficace e documentabile del rischio insito nel trattamento.

"GDPR NUOVA PRIVACY - LA CONFORMITÀ SU MISURA" offre un prezioso supporto in questo senso a tutti gli operatori che si trovano ad affrontare l'implementazione del Regolamento: titolari, responsabili, *compliance manager, data privacy officer* ma anche auditor e consulenti, tanto professionisti quanto imprese.

Fulcro dell'opera è infatti il percorso con cui gli Autori – competenti ed autorevoli esperti di *governance* della sicurezza ICT e privacy – accompagnano il lettore attraverso la costruzione di un "approccio strutturato" per la realizzazione della propria personale gestione del Regolamento, sviluppando ed offrendo un modello di riferimento basato sull'organizzazione, secondo una sequenza logica, di un numero circoscritto di gruppi di funzioni che costituiscono i pilastri fondamentali per l'attuazione di un'efficace gestione del rischio connesso al trattamento di dati personali, cuore della *compliance.*

Ciascuna funzione viene collocata all'interno del gruppo di riferimento e coordinata con gli altri elementi ad essa appartenenti, e ciascun gruppo con gli altri gruppi di funzione: questa base, anche associata alle eventuali prassi, standard e linee guida già adottate dal singolo titolare, consente di sviluppare una strategia di gestione del rischio coerente con il principio di *privacy by design e by default*.

Il modello è inoltre arricchito dalla individuazione analitica degli strumenti per la sua concreta attuazione, costituiti sia da documentazione originale appositamente predisposta dagli Autori, sia da un amplissimo parco di documenti acquisiti da fonti esterne ufficiali, tutti a disposizione del lettore in formato cartaceo e – ove disponibile il formato elettronico – sul sito dell'Editore.

Utile sotto il profilo pratico si rivela anche la scelta di raggruppare gli articoli e i *considerando* del Regolamento attinenti ad un medesimo tema, ponendoli inoltre a diretto confronto con le analoghe norme dell'attuale Codice Privacy e alcuni rilevanti provvedimenti del Garante: in questo modo si rende con immediatezza al lettore il completo panorama normativo di riferimento sul tema specifico di interesse, evidenziando le differenze (di approccio, di principio e di dettaglio) tra vecchio e nuovo sistema, che vengono comunque affrontate anche in modo più sistematico nella seconda parte del libro, mediante lo strumento dell'esemplificazione basata su specifici casi di trattamento.

Un'opera, insomma, dai molti pregi, caratterizzata da un approccio concreto e innovativo alla materia, che compendia in modo analitico ed organizzato lo stato dell'arte su norme, processi, linee guida e altri materiali provenienti dalle fonti più disparate, e nel contempo un'opera ricca di contenuti originali che costituiscono ben più che semplici spunti di riflessione; un'opera per la quale mi sento di ringraziare gli Autori, che hanno messo con grande professionalità a disposizione del pubblico, in modo pienamente fruibile, il frutto di una lunghissima e qualificata esperienza.

Maria Roberta Perugini *

* *Avvocato, partner di Jacobacci & Associati, di cui dirige la divisione data protection. Ha maturato una particolare ed approfondita esperienza in materia di tutela della privacy, settore nel quale opera sin dal 1995 fornendo ad imprese e gruppi anche multinazionali, attivi nei più svariati settori di mercato, consulenza sia per la compliance sia per lo sviluppo di progetti speciali in questa materia, correntemente integrata dall'assistenza sui connessi profili contrattuali e più prettamente civilistici.*
Partecipa come relatrice a convegni in materia di protezione dei dati personali ed organizza eventi e seminari volti a consolidare ed ampliare la conoscenza e consapevolezza da parte del mercato delle problematiche di data protection, nonché workshop di formazione ed aggiornamento presso imprese e associazioni di categoria. Redige e divulga note di aggiornamento e riflessione su problematiche attuali di data protection e contribuisce a europrivacy.info.

Questo libro è ottimo per tempestività, completezza, approfondimento e chiarezza. Già nel titolo il riferimento alla conformità "su misura" esemplifica efficacemente l'effetto fondamentale del sistema giuridico configurato dal GDPR, che è quello di spingere il titolare verso la costruzione del proprio personale percorso di conformità del trattamento alle norme: conformità che coincide in concreto con una prevenzione adeguata, efficace e documentabile del rischio insito nel trattamento.

Il libro offre un prezioso supporto in questo senso a tutti gli operatori che si trovano ad affrontare l'implementazione del Regolamento: titolari, responsabili, *compliance manager, data privacy officer* ma anche auditor e consulenti, tanto professionisti quanto imprese. Fulcro dell'opera è infatti il percorso con cui gli Autori – competenti ed autorevoli esperti di *governance* della sicurezza ICT e privacy – accompagnano il lettore attraverso la costruzione di un "approccio strutturato" per la realizzazione della propria personale gestione del Regolamento, sviluppando ed offrendo un modello di riferimento basato sull'organizzazione, secondo una sequenza logica, di un numero circoscritto di gruppi di funzioni che costituiscono i pilastri fondamentali per l'attuazione di un'efficace gestione del rischio connesso al trattamento di dati personali, cuore della *compliance*.

Ciascuna funzione viene collocata all'interno del gruppo di riferimento e coordinata con gli altri elementi ad essa appartenenti, e ciascun gruppo con gli altri gruppi di funzione: questa base, anche associata alle eventuali prassi, standard e linee guida già adottate dal singolo titolare, consente di sviluppare una strategia di gestione del rischio coerente con il principio di *privacy by design* e *by default*. Il modello è inoltre arricchito dalla individuazione analitica degli strumenti per la sua concreta attuazione, costituiti sia da documentazione originale appositamente predisposta dagli Autori, sia da un amplissimo parco di documenti acquisiti da fonti esterne ufficiali, tutti a disposizione del lettore in formato cartaceo e – ove disponibile il formato elettronico – sul sito dell'Editore.

Utile sotto il profilo pratico si rivela anche la scelta di raggruppare gli articoli e i *considerando* del Regolamento attinenti ad un medesimo tema, ponendoli inoltre a diretto confronto con le analoghe norme dell'attuale Codice Privacy e alcuni rilevanti provvedimenti del Garante: in questo modo si rende con immediatezza al lettore il completo panorama normativo di riferimento sul tema specifico di interesse, evidenziando le differenze (di approccio, di principio e di dettaglio) tra vecchio e nuovo sistema, che vengono comunque affrontate anche in modo più sistematico nella seconda parte del libro, mediante lo strumento dell'esemplificazione basata su specifici casi di trattamento.

Un'opera, insomma, dai molti pregi, caratterizzata da un approccio concreto e innovativo alla materia, che compendia in modo analitico ed organizzato lo stato dell'arte su norme, processi, linee guida e altri materiali provenienti dalle fonti più disparate, e nel contempo un'opera ricca di contenuti originali che costituiscono ben più che semplici spunti di riflessione; un'opera per la quale mi sento di ringraziare gli Autori, che hanno messo con grande professionalità a disposizione del pubblico, in modo pienamente fruibile, il frutto di una lunghissima e qualificata esperienza.

Avv. Maria Roberta Perugini

Giancarlo Butti *(LA BS 7799), (LA ISO IEC 27001), CRISC, ISM, DPO, CBCI, AMBCI* - Project manager, security manager ed auditor presso gruppi bancari, consulente in sicurezza e privacy presso aziende di diversi settori e dimensioni. Ha all'attivo oltre 700 articoli, 20 libri, 6 opere collettive. È membro della faculty di ABI Formazione e docente presso altre istituzioni. È socio e proboviro di AIEA/ISACA e socio del CLUSIT. Partecipa a numerosi gruppi di lavoro (ABI, UNINFO, ISACA…) in materia di sicurezza e privacy. Fra i coordinatori di www.europrivacy.info.

Alberto Piamonte - Laureato in Ingegneria Elettronica, fa parte del KeyMap Team, un gruppo che si occupa dello sviluppo di strumenti automatizzati e metodologie per attività di audit, l'analisi e gestione dei rischi, la certificazione conformità e la realizzazione di efficaci ed efficienti sistemi di controllo e di governo. Consulente sul governo dei sistemi IT, tiene corsi e seminari su metodologie quali COBIT, ITIL e ISO27001. Già Consigliere AIEA con il ruolo di Research Director è ora socio di ISACA Roma, COBIT5 Trainer, Assessor ed Implementor.

Maria Roberta Perugini - Avvocato, partner di Jacobacci & Associati, di cui dirige la divisione data protection, settore nel quale opera professionalmente sin dal 1995. Relatrice a convegni, organizza eventi e seminari e workshop. Redige e divulga note di aggiornamento e riflessione su problematiche attuali di data protection e contribuisce a www.europrivacy.info.

ISBN 9788890341915

Prezzo € 34