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

PRINCIPI

I PRINCIPI DELLA PROTEZIONE DEI DATI PERSONALI

Articolo UE 2016/679	Note	Cons.
5 - Principi applicabili al trattamento di dati personali	1. I dati personali sono: a. trattati con "liceità, correttezza e trasparenza"; b. raccolti per finalità determinate, esplicite e legittime; c. adeguati, pertinenti e limitati; d. esatti e, se necessario, aggiornati; e. per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; f. trattati in maniera da garantire un'adeguata sicurezza. 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione": accountability).	39

Articolo 5 - Principi applicabili al trattamento di dati personali

1. I dati personali sono:
   a) trattati in modo **lecito**, **corretto** e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); *[11 a]*

   b) raccolti per finalità **determinate**, **esplicite** e **legittime**, e successivamente trattati in modo che non sia in**compatibile con tali finalità**; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); *[11 b]*

   c) **adeguati**, **pertinenti** e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); *[11 c]*

   d) **esatti** e, se necessario, **aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); *[11 c]*

   e) **conservati in una forma che consenta l'identificazione degli interessati** per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini

statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da **trattamenti non autorizzati o illeciti** e dalla **perdita, dalla distruzione o dal danno accidentali** («integrità e riservatezza»). *[31]*

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Normativa previgente - Articolo 5

Articolo 11

Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:

   a) trattati in modo **lecito** e secondo **correttezza**;

   b) raccolti e registrati per scopi **determinati, espliciti** e **legittimi**, ed utilizzati in altre operazioni del trattamento in termini **compatibili con tali scopi**;

   c) **esatti** e, se necessario, **aggiornati**;

   d) **pertinenti, completi** e **non eccedenti** rispetto alle finalità per le quali sono raccolti o successivamente trattati;

   e) **conservati in una forma che consenta l'identificazione dell'interessato** per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati

Articolo 31

Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i **rischi di distruzione o perdita, anche accidentale**, dei dati stessi, di **accesso non autorizzato o di trattamento non consentito o non conforme** alle finalità della raccolta.

Considerando

39 Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento.

In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

Sanzioni

Amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

RAPPORTO CON LA NORMATIVA ESISTENTE

Anche l'attuale normativa richiede la presenza di POLICY, PROCESSI, DOCUMENTI…

Tuttavia vi è una sostanziale differenza fra il D.Lgs 196/03 ed il GDPR.

L'approccio del Codice Privacy

Il D.Lgs 196/03 richiede la formalizzazione esplicita solo di un limitato insieme di DOCUMENTI e di MISURE TECNICHE ed ORGANIZZATIVE.

In modo esplicito il D.Lgs 196/03 richiede che siano prodotte:

- INFORMATIVE
- LETTERE DI INCARICO E DESIGNAZIONE ED ELENCHI DEI SOGGETTI DESIGNATI
- ISTRUZIONI SCRITTE

nonché che siano implementate una serie di misure minime di sicurezza, relative in alcuni casi ad aspetti tecnici, quali ad esempio l'uso di un antivirus o aspetti organizzativi, quali la verifica periodica dell'elenco dei soggetti autorizzati al trattamento.

Non richiede una reale formalizzazione di policy e procedure, in quanto si limita a valutare il risultato.

Parti di normativa che richiedevano la formalizzazione di aspetti significativi quali un'analisi dei rischi o una mappatura esplicita dei trattamenti sono stati nel tempo aboliti (DPS) in quanto erroneamente interpretati come meri adempimenti formali e non già come un prerequisito indispensabile al rispetto della normativa nel suo insieme.

Nel suo complesso quindi il D.Lgs 196/03 richiede solo l'esistenza implicita di prassi o procedure che permettano il rispetto della stessa, ma non la loro formalizzazione.

Un sistema di gestione della privacy basato sul D.Lgs 196/03 è quindi costituto nella maggior parte dei casi da un apparato documentale costituito da documenti espressamente previsti dalla normativa (informative ed incarichi) e non anche da procedure che ne descrivano la modalità di formalizzazione e d'uso.

Lo stesso apparato sanzionatorio del resto è basato per lo più sulla violazione di aspetti formali, quali la omessa o inadeguata informativa, l'omessa notificazione, l'omessa adozione di misure minime di sicurezza che su una reale gestione della privacy.

L'APPROCCIO DEL GDPR

L'approccio del GDPR, e questa è una delle più rilevanti novità, è decisamente diverso.

Il GDPR non si limita a valutare i risultati formali, che spesso non sono nemmeno definiti (non esiste ad esempio un elenco di misure minime), ma si focalizza sul processo in atto per presidiare la privacy nell'organizzazione.

Al riguardo l'articolo 24 evidenzia la necessità, in capo al titolare, di essere in grado di **dimostrare** per esteso (cioè per ogni disposizione del Regolamento) come i trattamenti siano conformi allo stesso.

GDPR

Articolo 24 Responsabilità del titolare del trattamento

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.

…

Ancor più incisivo l'articolo 5 che richiede allo stesso titolare la capacità di comprovare la propria capacità di rispettare i principi in esso stabiliti.

GDPR

Articolo 5 Principi applicabili al trattamento di dati personali

…

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

…

Ne consegue che ciò che va dimostrato in molti casi non è un risultato, ma una policy od un processo.

Il livello di formalizzazione richiesto è quindi molto più spinto e l'incapacità di **comprovare** ad esempio il rispetto dell'articolo 5 espone alle più gravi sanzioni.

GDPR

Articolo 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie

…

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

…

Vi è quindi una sostanziale differenza fra l'approccio delle due normative, che si riflette anche in quelli che potrebbero apparire semplice diverse modalità di presentazione di un risultato.

In realtà tuttavia il rispetto del D.Lgs 196/03 ed il rispetto del GDPR si basano necessariamente sulla formulazione di un rilevante numero di policy e procedure, che nel caso del D.Lgs 196/03 sono per lo più espresse come prassi.

Esempio: INFORMATIVA

Approccio

Il D.Lgs 196/03 prevede nella sua parte generale uno specifico articolo relativamente all'informativa da rilasciare agli interessati, indipendentemente che i dati siano raccolti presso l'interessato o presso terzi:

D.Lgs 196/03

ART. 13 INFORMATIVA

…

mentre il GDPR declina questi 2 casi con specifici articoli:

GDPR

Articolo 13 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

…

Articolo 14 Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

…

Contenuti

Relativamente ai contenuti le informative previste dal D.Lgs 196/03 e dal GDPR differiscono in diversi punti.

Il testo evidenzia le possibili concordanze di contenuti fra le 2 norme e le parti previste da una delle normative e non dall'altra.

D.Lgs 196/03	UE 2016/679 (GDPR)
ART. 13 INFORMATIVA	*Articolo 13* - **Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato** *Articolo 14* - **Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato**
1 L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:	1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
f) gli **estremi identificativi del titolare** e, se designati, del **rappresentante** nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile	a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

STRUMENTI PER MAPPARE PROCESSI E TRATTAMENTI

(Tratto da G.Butti - Sicurezza Totale/Dalla carta alle nuvole – Iter srl)

La rilevazione dei processi aziendali

All'interno di un'azienda, le attività sono organizzate in processi più o meno strutturati e ripetitivi, indipendentemente dal fatto che si tratti di un'azienda manifatturiera, commerciale o di servizi.

Un processo consente, attraverso le conoscenze, le competenze, i sistemi, gli strumenti, di arrivare ad un risultato definito.

In genere tutti i processi aziendali comportano un trattamento di dati personali, fossero anche solo quelli relativi ai soggetti che sono preposti alla loro conduzione.

Le definizioni di processo sono diverse:

- una serie di attività che trasformano uno o più input in uno o più output
- una concatenazione di attività che portano ad ottenere il prodotto/servizio richiesto
- un insieme di attività, tra di loro correlate da legami di precedenza, che devono raggiungere un determinato obiettivo
- un insieme di compiti individuali che vengono uniti per completare una transazione (cioè un processo di business chiaramente identificabile) all'interno dell'impresa.

Più precisamente possiamo definire come processo una serie di una o più procedure o attività collegate che collettivamente realizzano un obiettivo aziendale, generalmente entro il contesto di una struttura organizzativa che definisce i ruoli funzionali e le relazioni.

Una possibile classificazione dei processi è legata alla loro finalità:

- processi che sono finalizzati alla generazione del business aziendale (quelli che producono l'utile dell'azienda)
- processi di servizio, spesso legati all'ambito amministrativo, come ad esempio la contabilità o la fatturazione
- processi tesi a definire le strategie aziendali o ad individuare nuovi prodotti.

I processi che competono alle diverse aree sono molto diversi fra loro, non solo come finalità, ma anche come impostazione.

I processi che riguardano l'area amministrativa ad esempio, al di là delle diversità presenti nelle varie aziende, sono molto ben definiti.

Alcuni aspetti di tali processi sono anche regolati dal punto di vista normativo. La loro definizione è talmente precisa che esistono da lungo tempo applicazioni software specifiche per poterli gestire. Ad esempio l'emissione di fatture, tratte e bonifici, avviene secondo una sequenza prestabilita e talmente consolidata da essere congelata nelle applicazioni informatiche di contabilità.

Ciò che differenzia i vari tipi di processo riguarda (ad esempio):

- una maggiore o minore strutturazione
- una maggiore o minore rigidità (possibilità di intervento da parte degli operatori per modificare il processo)
- una maggiore o minore prevedibilità

- una maggiore o minore ripetitività nel tempo
- l'uso di informazioni e documenti ben determinati o viceversa legati al contesto specifico.

I processi di produzione in serie ad esempio, sono generalmente caratterizzati da una elevata strutturazione, sono molto ben definiti e ripetitivi; schemi prefissati guidano completamente l'operatore nello svolgimento della sua attività.

Tutti gli elementi, informazioni, strumenti, componenti, materiali, che servono per la realizzazione del processo, vengono forniti all'operatore in forma più o meno automatizzata.

Altri processi sono invece legati prevalentemente alla capacità di intervento dei singoli operatori. Possono variare gli elementi che servono alla realizzazione del processo e sono gli stessi operatori a procurarsi quelli che ritengono più utili per svolgere la propria attività.

Esempi di processo di questo tipo sono la definizione di un nuovo prodotto o la realizzazione di uno stampo; si tratta di processi nei quali è richiesto l'intervento di operatori con conoscenze e competenze specifiche.

Nella realtà esistono ovviamente tipi di processo che si collocano fra questi due estremi.

I componenti dei processi

I processi sono costituiti da una serie di attività, che possono essere svolte sequenzialmente o parallelamente.

Un'attività può essere costituita da un form da compilare, un documento da approvare, una telefonata da fare, un pezzo da assemblare…

Un'attività può essere svolta unicamente quando sono disponibili tutti gli elementi utili alla sua esecuzione, ed il risultato ottenuto dal suo svolgimento costituisce l'input per l'attività successiva.

Le attività

L'attività costituisce l'unità di base con cui viene descritto un processo. Per il suo svolgimento l'attività passa attraverso tre diverse condizioni principali:

- per partire devono essere soddisfatte tutte le condizioni imposte per la sua attivazione; queste possono riguardare:
    - disponibilità di documenti
    - disponibilità di informazioni
    - disponibilità di strumenti
    - disponibilità di componenti
    - disponibilità di materie prime e semilavorati
    - verificarsi di eventi
    - assunzione del giusto valore da parte di alcuni parametri
    - ….
- una condizione operativa, che identifica l'attività nel corso del suo svolgimento. In questa fase chi compie l'attività, attraverso regole precise e con gli strumenti ed il materiale che ha a disposizione, compie azioni definite, nel tempo stabilito, per ottenere un risultato prestabilito
- una condizione finale dove, in base alle azioni svolte ed ai risultati conseguiti, vengono aggiornati i parametri iniziali. Nel corso dello svolgimento dell'attività possono verificarsi diversi eventi che determinano il raggiungimento o meno del risultato finale, nonché quale sia l'attività da

svolgere successivamente a quella in corso. Ad esempio il risultato finale può non essere raggiunto perché nel corso dell'attività è venuto meno uno dei componenti richiesti al suo svolgimento.

Esempi e schede di rilevazione di un processo

Per le finalità di questo libro, relativamente ad un processo è opportuno rilevare:

- le informazioni utilizzate (compresi i dati personali)
- dove queste sono conservate (sistema informativo, documenti, supporti magnetici...)
- le strutture coinvolte
- gli strumenti utilizzati
- le attività svolte.

La scheda riportata è pensata per rilevare le attività di una singola unità organizzativa per volta, mappando per le varie attività anche le controparti coinvolte (unità organizzative interna all'azienda o anche entità esterne alla stessa).

La rilevazione consente di censire:

- strumenti
- attività

Strumento	**Descrizione attività/Risultato atteso**

e successivamente nel dettaglio:

- strumenti utilizzati
- dati utilizzati (a livello macro)
- operazioni effettuate
- controparti interessate (IN/OUT).

Per mappare le varie attività dell'ufficio si compila una scheda per ogni singolo processo.

Descrizione attività											
Supporto informazione											
Elettronico											
Cartaceo											
Strumenti											
Controparte											
IN/OUT											

Esempio

In questo esempio, sono censiti alcuni processi svolti in uno studio di commercialista nell'ambito della gestione della CONTABILITÀ ORDINARIA. La modalità di rilevazione è in questo caso effettuata ufficio per ufficio e per macro attività; quindi uno degli elementi (gli operatori coinvolti) è predeterminato. Questa modalità di descrizione dei processi è legata anche alla modalità di raccolta delle informazioni, che può avvenire mediante interviste al responsabile dell'ufficio.

Descrizione Attività	Smistamento Documenti	Elaborazione Prima Nota Codifica Fatture	Dettagli Contabili	Elaborazione Bilancio	Stampa Schede + Controllo	Stampa Giornale + Mastri per Consegna	Lettere Reso Documenti Co/Ge	Libro Cespiti	Stampa Libro Cespiti		Verbali Societari Preparazione	Aggiornamento Libri Sociali + Consegna	Archiviazione Copie
Supporto informazione													
Elettronico		X	X	X	X	X		X	X		X	X	X
Cartaceo	X			X	X	X	X	X	X			X	X
Strumenti		**DB COGE**	**ELABORATORE TESTI FOGLIO ELETTRONICO**	**DB COGE +ARCHIVIO II**	**ARCHIVIO CONT.+ ARCHIVIO INGRESSO**			**DB COGE**	**ARCH.UFF.CONT.+ ARCH.INGRESSO**		**ELABORATORE TESTI**		**ARCH. IVA+ ARCH. SEGRETERIA**
Controparte	**AZIENDA**					**AZIENDA CLIENTE**	**AZIENDA CLIENTE**					**AZIENDA CLIENTE**	
IN/OUT	**IN**					**OUT**	**OUT**					**OUT**	

Strumento	**Descrizione attività/Risultato atteso**
Posta elettronica	Verbali - Bilanci - Relazioni Collegio Sindacali - Cda
Navigazione Internet	Agenzia Entrate
Elaboratore testi	Verbali - Bilanci - Lettere Comunicazioni
Foglio elettronico	Dettagli Contabili
Procedura contabile	Contabilità generale + Libro Cespiti

La rilevazione dei flussi documentali

Il metodo descritto in queste pagine consente di mappare i flussi documentali di un processo o di un'intera azienda.

In questo modo è possibile identificare quali sono i documenti prodotti e ricevuti da una specifica unità organizzativa aziendale e conseguentemente quali sono le unità organizzative che partecipano ad un determinato trattamento di dati personali.

Le unità organizzative interne all'azienda (o soggetti anche esterni ad essa) sono collocate secondo una linea obliqua e sono rappresentate da dei rettangoli.

I documenti prodotti e scambiati con altre unità organizzative sono rappresentati da altri rettangoli, più stretti in altezza dei precedenti. Un documento che viene inoltrato dall'Ufficio 1 all'Ufficio 2, verrà posizionato sulla stessa linea orizzontale dell'ufficio emittente e sulla linea verticale dell'ufficio ricevente.

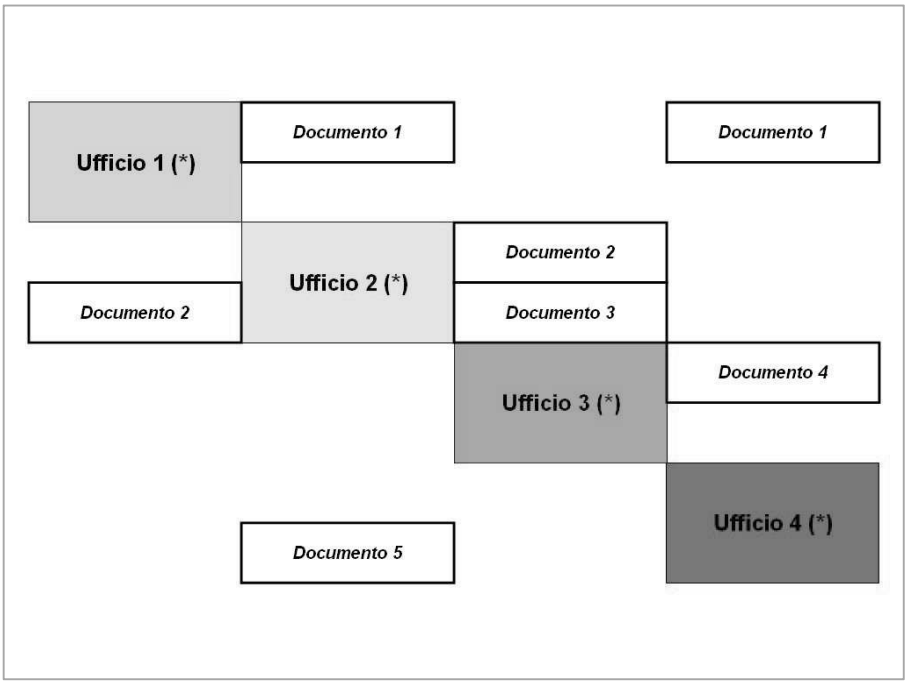
Se lo stesso documento viene inviato a più uffici, sarà riportato più volte sulla linea orizzontale in corrispondenza degli uffici destinatari.

L'ufficio destinatario può sia precedere sia seguire l'ufficio emittente sulla linea obliqua:

- nel caso in cui segua l'ufficio emittente, il simbolo del documento verrà posizionato in alto rispetto al simbolo dell'ufficio
- nel caso in cui preceda l'ufficio emittente, il simbolo del documento verrà posizionato in basso rispetto al simbolo dell'ufficio.

Il posizionamento delle varie strutture aziendali sulla linea obliqua deve essere in linea di massima effettuato con una logica sequenziale rispetto al processo che si sta esaminando.

Tuttavia la possibilità di indicare come destinatari dei documenti sia le unità organizzative che precedono sulla linea obliqua, sia quelle che seguono, rende di fatto molto flessibile l'uso di tale rappresentazione.



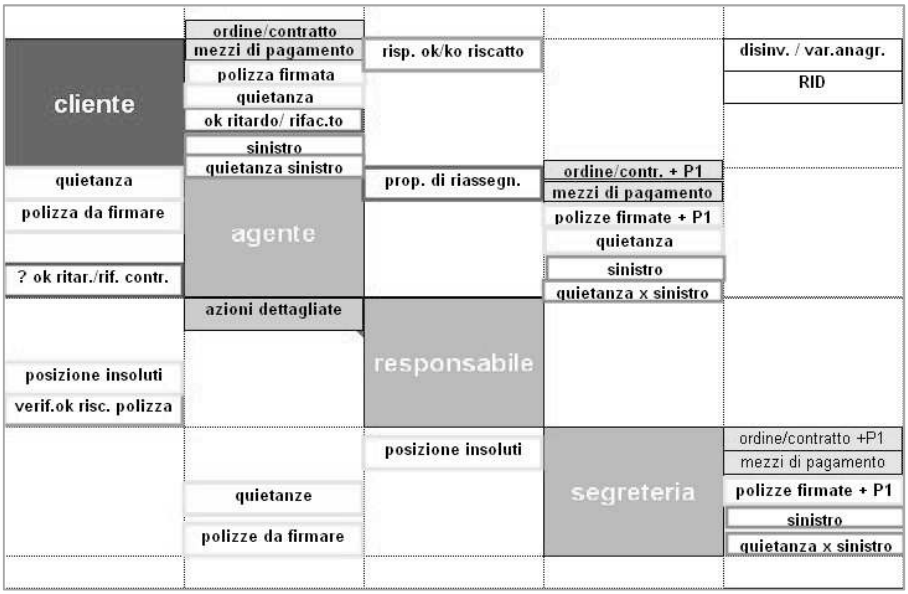
L'uso di tale metodologia può avvalersi di apposite macro implementabili in fogli elettronici oppure mediante l'uso di cartoncini colorati rimuovibili da utilizzare su una lavagna.

L'esempio che viene riportato riguarda uno stralcio dell'analisi del flusso di documenti in un processo di gestione di polizze assicurative.

Grazie a questa rappresentazione è possibile individuare tutte le unità organizzative che partecipano al trattamento e, se l'analisi è sufficientemente dettagliata, quale tipologia di dati personali sono trattati dalla singola unità per una certa categoria di interessati.

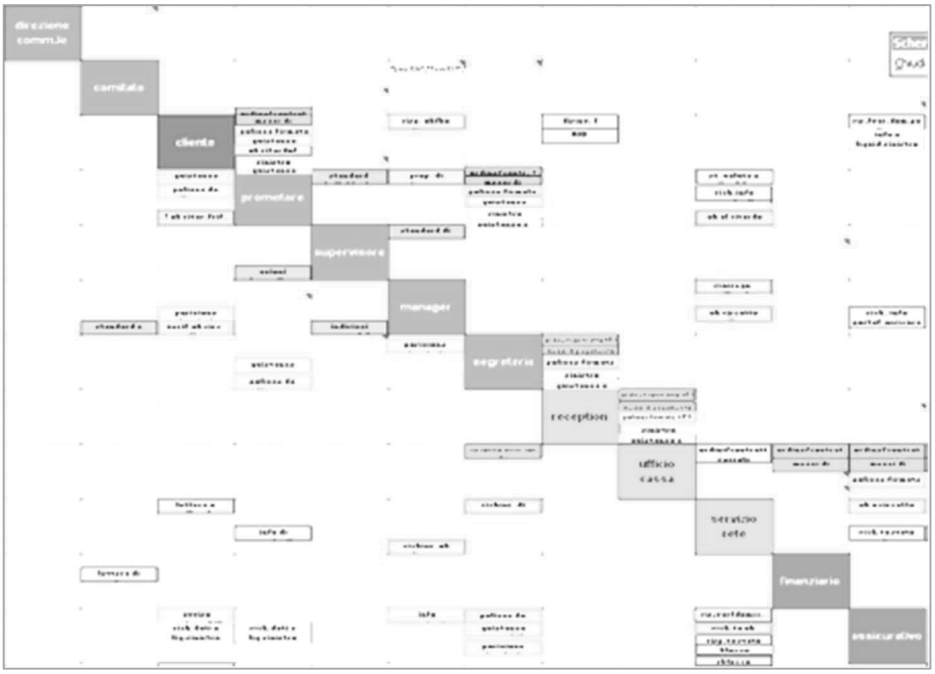
I documenti scambiati dal cliente con i vari soggetti aziendali sono relativi ad esempio:

- alla sottoscrizione del contratto
- al pagamento della polizza
- alla denuncia di un sinistro.



L'analisi si può estendere all'intera azienda coinvolgendo le varie unità organizzative e mappando quindi lo scambio di documenti ed eventualmente anche altre azioni.

L'analisi può essere estesa anche all'esterno dell'azienda, individuando quindi i soggetti che partecipano al trattamento.


direzione comm.le
cliente
promotore
supervisore
manager
segreteria
reception
ufficio cassa
servizio rete
finanziario
assicurativo

ESEMPIO 3

Regole per le comunicazioni aziendali da e verso l'esterno

Tipologia di comunicazioni	Le comunicazioni dell'azienda possono avvenire sia in uscita, sia in ingresso. L'azienda prevede principalmente le seguenti tipologie di comunicazioni: • comunicazioni che impegnano contrattualmente l'azienda • comunicazioni di natura fiscale • comunicazioni di servizio • comunicazioni specificatamente regolamentate • comunicazioni di cortesia • comunicazioni pubblicitarie Esempi • comunicazioni che impegnano contrattualmente l'azienda o ordini in ingresso ed uscita • comunicazioni di natura fiscale o DDT, fatture • comunicazioni di servizio (si intendono tutte le comunicazioni che precedono la formalizzazione di un ordine e/o di un contratto e, successivamente allo stesso, ne consentano la gestione) o richieste di offerte o gestione di progetti o solleciti, diffide o convocazioni di riunioni • comunicazioni di cortesia o auguri • comunicazioni specificatamente regolamentate (in quanto previste contrattualmente) o richieste di intervento o interazione con clienti e fornitori per la gestione di un progetto o di una fornitura • comunicazioni pubblicitarie

Strumenti per la comunicazione:	L'azienda prevede principalmente le seguenti modalità di comunicazione:
	• posta cartacea
	  ○ ordinaria
	  ○ raccomandata
	  ○ assicurata
	• telegramma
	• posta elettronica
	  ○ ordinaria messaggi
	  ○ ordinaria con documenti allegati
	• PEC
	• Fax
	• Telefono
	• SMS ed MMS

Valore civilistico e fiscale delle comunicazioni	Ai sensi degli articoli del Codice Civile (Artt. 2214 e 2220) e del D.P.R. 600/73 (Art. 22) le comunicazioni che hanno valore commerciale e/o fiscale devono essere conservate per 10 anni.

L'uso degli strumenti di comunicazione è ammesso secondo la seguente tabella

	Impegno contrattuale	**Fiscale**	**Servizio**	**Regolamentata**	**Cortesia**	**Pubblicitaria**
POSTA CARTACEA						
Ordinaria	✓	✓	✓	✓		✓
Raccomandata	✓		✓	✓		
Assicurata						
Telegramma						
POSTA ELETTRONICA						
Ordinaria messaggi			✓	✓	✓	✓
Ordinaria allegati	✓	✓	✓	✓	✓	✓
PEC	✓	✓		✓		
FAX	✓	✓	✓	✓	✓	✓
TELEFONO			✓	✓	✓	
SMS ed MMS			✓	✓	✓	✓

Enti autorizzati alle comunicazioni esterne (in uscita)

	Tipo documento	**Struttura interessata**
COMUNICAZIONI CHE IMPEGNANO CONTRATTUALMENTE L'AZIENDA		
	Ordini vs. fornitori	Acquisti
	Conferme d'ordine	Commerciale
	Ddt	Spedizioni
COMUNICAZIONI FISCALI		
	Fiscali	Contabilità clienti/fornitori
COMUNICAZIONI DI SERVIZIO		
		Tutte le strutture coinvolte
COMUNICAZIONI SPECIFICATAMENTE REGOLAMENTATE		
		Tutte le strutture coinvolte
COMUNICAZIONI DI CORTESIA		
		Tutte le strutture coinvolte
COMUNICAZIONI PUBBLICITARIE		
	Generiche/massive	Mkt
	Su richiesta	Commerciale

Enti destinatari delle comunicazioni (in entrata)

	Tipo documento	**Struttura interessata**
COMUNICAZIONI CHE IMPEGNANO CONTRATTUALMENTE L'AZIENDA		
	Ordini da clienti	Commerciale
	Ddt	Acquisti
COMUNICAZIONI FISCALI		
	Fiscali	Contabilità clienti/fornitori
COMUNICAZIONI DI SERVIZIO		
		Tutte le strutture coinvolte
COMUNICAZIONI SPECIFICATAMENTE REGOLAMENTATE		
		Tutte le strutture coinvolte

	Tipo documento	**Struttura interessata**
COMUNICAZIONI DI CORTESIA		
		Tutte le strutture coinvolte
COMUNICAZIONI PUBBLICITARIE		
		Spedizioni per smistamento

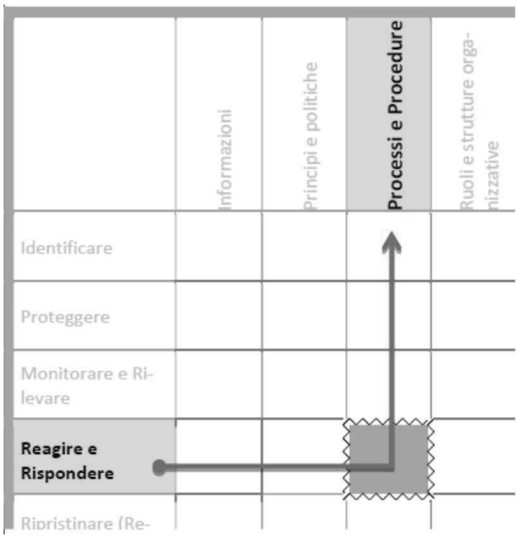
Livelli di sicurezza nelle comunicazioni – classificazione

Livello di sicurezza	**Alto**	**Medio**	**Basso**
Livello di confidenzialità	**Riser-vato**	**Interno**	**Pub-blico**
Tipo documento			
Tutti i documenti: • che impegnano contrattualmente l'azienda • che riguardano trattative in corso con clienti e fornitori • che riguardano la gestione di progetti per importi superiori a 10.000 euro.	✓		
Documenti che contengano dati personali sensibili o giudiziari.	✓		
Documentazione fiscale Tutti i documenti: • che impegnano contrattualmente l'azienda • che riguardano trattative in corso con clienti e fornitori • che riguardano la gestione di progetti per importi inferiori o uguali a 10.000 euro. Comunicazioni di servizio relative a progetti senza contenuto informativo (ad esempio semplice conferma di appuntamenti).		✓	
Materiale pubblicitario			✓

I PROCESSI E LE PROCEDURE

PROCESSI DI RISPOSTA AD EVENTI

Lo schema suggerito prevede che, in corrispondenza a determinati eventi, siamo in grado di rispondere in modo "attivo". Dobbiamo cioè essere capaci di reagire adottando una serie di azioni mirate ad un preciso obiettivo. Tali azioni non vanno "improvvisate", ma, sempre per il principio del "*by design*", dovranno essere state precedentemente preparate, pianificate ed organizzate definendo specifiche procedure. La conformità consiste non solo nell'agire, ma anche e soprattutto nell'essere preparati ed essere in grado di dimostrarlo.



Abbiamo già anticipato che tali procedure potranno essere definite:

1. Usando la propria esperienza ed il buon senso
2. Ispirandosi a documenti prodotti da qualche fonte autorevole (in particolare dalle Autorità di controllo)
3. Basandosi su standard o Framework disponibili sul mercato.

Nelle pagine seguenti abbiamo scelto due esempi significativi di **Processi di risposta ad eventi** prendendo spunto da fonti diverse ed esattamente:

Processo	Fonte	Caratteristiche principali
Risposta alle richieste dell'interessato	COBIT5 – Processo DS02 – Rispondere a incidenti e a richieste di servizio. ISACA (USA-Europa)	Il Framework COBIT5 costituisce un autorevole punto di riferimento in tema di Governance.
Risposta ad una violazione di dati (Data Breach)	Rielaborazione da fonti varie	

<table>
<tr><th colspan="2">SICUREZZA LOGICA</th></tr>
<tr><th>ASPETTI TECNICI</th><th>ASPETTI ORGANIZZATIVI E GESTIONALI</th></tr>
<tr><th colspan="2">CREDENZIALI DI AUTENTICAZIONE</th></tr>
<tr><td colspan="2">Misure tecniche ed organizzative per:
la gestione nel tempo delle credenziali di utenti e tecnici
la loro profilazione
la gestione di password o altri dispositivi di autenticazione.
Prerequisito per la definizione dei profili è:
l’identificazione degli asset accessibili
la definizione dei ruoli aziendali
la definizione dei privilegi di accesso
L’autenticazione consente di riconoscere un utente, mentre la corretta attribuzione di un profilo autorizzativo, consente di definire i limiti di accesso ed il tipo di azioni effettuabili sui dati e sui sistemi da parte di un utente.</td></tr>
<tr><td>Sistema di autenticazione
L’autenticazione dell’utente può avvenire in base a:
quello che si conosce:
password
PIN
quello che si possiede:
badge
token
one time password
quello che si è:
caratteristiche biometriche

Sistemi di autorizzazione
Profilatura accessi su sistemi ed applicativi
Partizione della rete</td><td>CREDENZIALI
Definizione dei profili coerenti con i ruoli
Divieto di creazione di profili ad personam
Definizione di una regola per la denominazione delle utenze
Assegnazione univoca delle credenziali ad ogni utente (compresi gli addetti alla configurazione e manutenzione dei sistemi)
Gestione delle credenziali nel tempo e verifica periodica
Disabilitazione in caso di perdita della qualità (esempio dimissioni)
Disabilitazione in caso di mancato utilizzo dopo un periodo stabilito o per assenza prolungata pianificata
Disabilitazione in caso di n tentativi errati di accesso
Disabilitazione al di fuori dell’orario lavorativo standard
Divieto di attribuzione della stessa credenziale a più di un incaricato
Divieto di uso di credenziali di gruppo (anche per utenze amministrative)
Istruzioni per la custodia delle credenziali
Attribuzione di diverse credenziali allo stesso utente se richiesto dai suoi ruoli
Divieto di uso delle utenze amministrative per lo svolgimento di operazioni per le quali è sufficiente l’uso di un'utenza “normale”

PASSWORD
Lunghezza minima commisurata al rischio
Regole nella costruzione
Mancanza di riferimenti agevolmente riconducibili all'incaricato
Segretezza della password</td></tr>
</table>

	Autonoma sostituzione al primo utilizzo Reset automatico della password di default dopo “x” tempo Sostituzione periodica Procedura per accesso ai dati anche in assenza dell'incaricato Eventuale comunicazione al Custode della password in forma segreta **UTENZE AMMINISTRATIVE** Assegnazione di credenziali personali ai singoli amministratori Disabilitazione delle utenze amministrative di default (ove possibile) Ridenominazione delle utenze amministrative di default (ove possibile) Divieto di uso delle utenze amministrative di default (ove possibile) **ACCESSO DA POSTAZIONI DIVERSE** Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse postazioni di lavoro **ACCESSO DIRETTO AI DATI** Impostazione dei profili di protezione in modo tale che non sia possibile accedere direttamente a dati o file senza passare dagli applicativi preposti, salvo che per attività di manutenzione ed in modalità controllata **CUSTODIA DELLO STRUMENTO** Istruzione agli incaricati per non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento
ANTI MALWARE	
Presenza di antivirus su tutte le postazioni Processo di aggiornamento Processo di scansione	Procedura in caso di allerta Procedura per la gestione di utility che possono bypassare le normali misure di sicurezza Divieto dell’uso di file o software non autorizzati
FIREWALL	
Firewall centralizzato/personale, adeguatamente configurato	Procedura di aggiornamento Procedura di monitoraggio Procedura in caso di allerta