COLIN
CONSULENTE LEGALE INFORMATICO

Le principali novità della General Data Protection Regulation

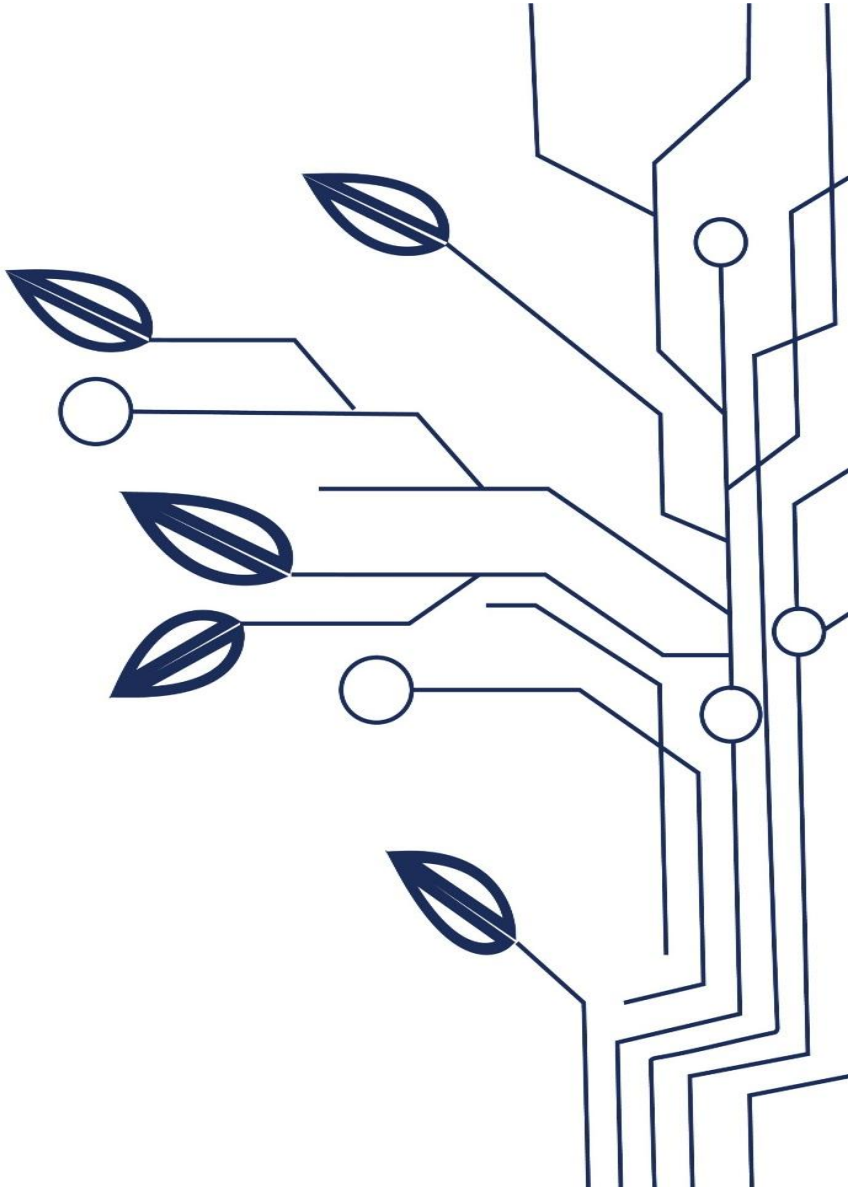
La normativa come scelta strategica

Avv. Alessandro Cecchetti

General Manager Colin & Partners

Bologna Business School

31 Marzo 2016

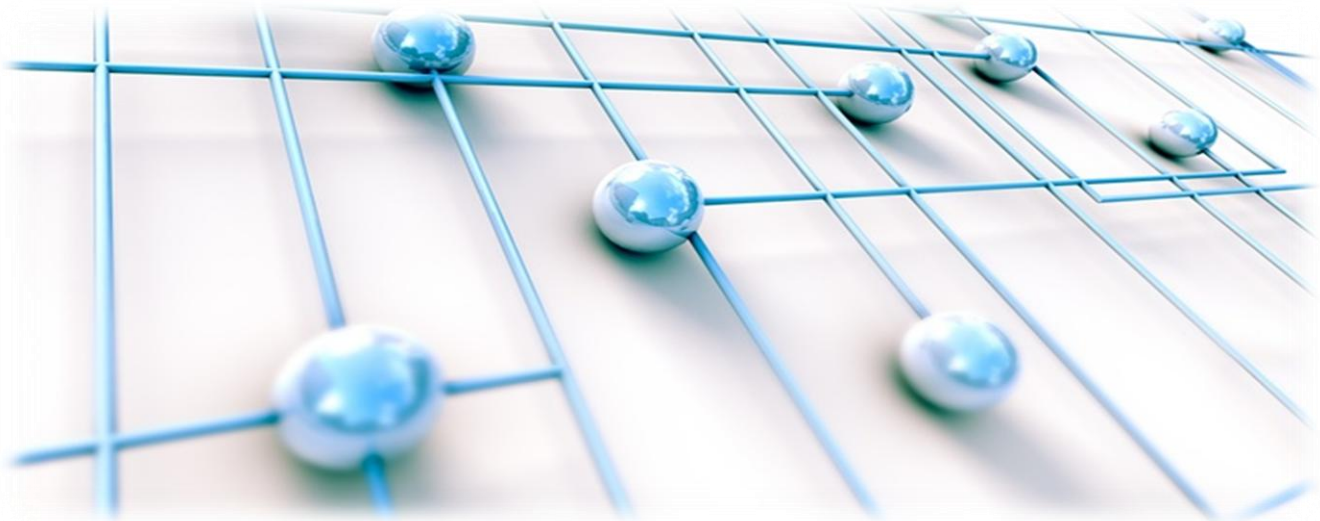


Colin & Partners

La nostra attività di consulenza si svolge nell'ambito del diritto delle nuove tecnologie e coinvolge aspetti di governance e reengineering dei processi interni, fino all'assistenza in fase di pre-contenzioso e contenzioso. Il supporto strategico del nostro team si caratterizza per un approccio assolutamente trasversale, teso a favorire l'ottimizzazione del business e delle esigenze del management aziendale.

Business Unit

- Diritto informatico
- Privacy & Tutela delle Informazioni
- Digitalizzazione
- Sorveglianza e controllo
- Modello 231 e reati informatici
- Intellectual property



OCSE a imprese e governi: considerare la sicurezza digitale un rischio economico

Il rischio per la sicurezza digitale dovrebbe essere considerato un **problema di ordine economico e non solo tecnologico, e dovrebbe essere integrato nei processi decisionali di ogni organizzazione**. Lo sostiene l'OCSE nella nuova **Raccomandazione sulla sicurezza digitale e la gestione del rischio** del 1 Ottobre 2015.

Un ambiente digitale globale, interconnesso, aperto e dinamico genera notevoli opportunità economiche, ancora più promettenti se si pensa alla crescente diffusione dell'Internet delle cose e dei Big Data. Tuttavia, Paesi e aziende sono esposti a minacce sempre più sofisticate e crescenti che possono mettere in pericolo la sicurezza delle informazioni e compromettere la prosperità economica e sociale.

In particolare, l'OCSE raccomanda **l'adozione di piani nazionali** per individuare le misure utili a prevenire, individuare, affrontare e sanare le conseguenze di incidenti di sicurezza digitale.

La Sicurezza delle Informazioni passa dal necessario **binomio** tecnologia + procedure. La compliance normativa deve essere riletta in un **senso utilitaristico**, ottimizzando le attività giornaliere, e fornendo un *quid pluris* all'azienda.

Alcuni concetti chiave introdotti dal Regolamento Europeo

Il principio dell'*Accountability*: le sanzioni previste possono arrivare fino al **4%** o a **20 milioni di €uro** del fatturato mondiale annuo di Gruppo

- **PIA e DATA BREACH**
- **IL DATA PROTECION OFFICER**
- **PRIVACY BY DESIGN**
- **OBBLIGHI CONTRATTUALI PER FORNITORI E SUBFORNITOR**

Tutela dati personali by design e by default

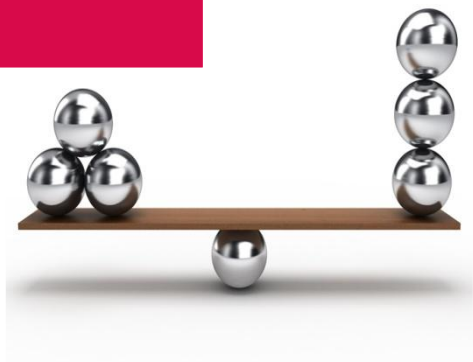
Viene introdotto l'obbligo di applicazione di entrambi i principi (by design e by defalut) , non escludendo uno l'applicazione dell'altro.

Privacy fin dalla progettazione

Minimizzazione e data retention

Sicurezza costante per l'intero ciclo vita dell'informazione

Trasparenza verso l'interessato/utente



DPO

Requisiti e posizione:

- Competenze legali;
- Competenze Informatiche
- Conoscenza del settore di mercato dove opera il Titolare o il Responsabile;
- Può essere interno o esterno, e può svolgere anche altri compiti;
- Non deve ricevere istruzioni in merito ai propri compiti e non può essere dimesso o penalizzato;
- Riferisce al CdA

DPO Compiti

Informare e consigliare il Titolare e il Responsabile e gli incaricati che trattano i dati personali circa i loro obblighi ai sensi della normativa in materia di protezione dei dati;

controllare il rispetto della normativa in materia di protezione dei dati e delle regole del Data Controller o Processor in materia di protezione dei dati personali;

fornire consulenza ove richiesto per quanto riguarda il P.I.A.: Privacy Impact Assessment e monitorare i relativi adempimenti;

cooperare con l'autorità di vigilanza (Autorità Garante Privacy);

agire come punto di contatto per l'autorità di vigilanza sulle questioni relative al trattamento dei dati personali. Deve prendere in debito considerazione i rischi associati alle operazioni di trattamento, avuto riguardo alla natura, allo scopo, al contesto ed alle finalità del trattamento.

Il Data Protection Officer

Per svolgere tali compiti deve avere un budget preventivamente stanziato e nel caso aggiornato, così come devono essere previsti degli aggiornamenti per il DPO.

Anche ai fini 231, sarà fondamentale la corretta formulazione del suo atto di nomina.

Per le Società a forte rilevanza tecnologica o con trattamenti particolari sarebbe opportuno prevedere più DPO con diverse competenze, assimilandone l'operato a quello dell'OdV.

Privacy Impact Assessment

Obbligo di PIA quando il trattamento

- venga effettuato con nuove tecnologie;
- presenta un rischio per i diritti e le libertà fondamentali dell'interessa-to
- Riguardi la profilazione;
- Riguardi categorie particolari di dati (es. biometrci)
- Riguardi la sorveglianza di zone accessibili al pubblico;
- Altre ipotesi decise e pubblicate dall'Autorità

Sentito il DPO, il Controller nella PIA deve tener conto degli impatti del trattamento sui diritti dell'interessato in un'ottica di adempimento agli obblighi del Regolamento anche relativamente all'operato dei fornitori e dei sub-fornitori, tenuto conto dei Pareri dei WP29.

Il rapporto tra il Controller, i Fornitori/Processors ed i sub-Fornitori/ sub-processors

Se, quando e come è lecito l'operato del sub-fornitori quando:

- Il Controller abbia dato il consenso scritto, specifico o generico;
- Il Processor deve aggiornare il Controller del variare dei sub-fornitori, dando la possibilità al Controller di obiettarvi;
- Il fornitore deve obbligare contrattualmente il sub-fornitore agli stessi obblighi assunti con il controller.

N.B. Qualora il sub fornitore ometta di adempiere ai propri obblighi, sarà comunque il fornitore a mantenere l'intera responsabilità dell'adempimento nei confronti del Controller

Notifica data breach ad Autorità competente/interessato

Gli obblighi di notifica seguente a data breach vengono estesi a qualsiasi caso in cui vi sia violazione dei dati personali. Viene poi esteso l'obbligo di darne comunicazione all'interessato nel caso in cui vi sia rischio elevato per i diritti e le libertà dello stesso. I tempi di comunicazione sono vaghi (*undue delay*). Rimangono comunque esclusi:

I casi in cui il controller abbia reso non comprensibili (leggi cifrati) i dati personali trattati

I casi in cui il controller abbia preso misure sufficienti ed idonee ad assicurare che i rischi non si verifichino

I casi in cui la comunicazione singola richieda l'utilizzo di risorse eccessivo; in questo caso ci dovrà essere una comunicazione pubblica

Societas delinquere non potest?
La 231 e i reati informatici

Accesso abusivo a sistema informatico rilevante ex 231

Tizio si introduce nel sistema informatico della Società per cui lavora per effettuare operazioni che portino un interesse o in vantaggio per la Società. Es.:

- accesso all'amministrazione modificare il credito dei clienti,
- maggiorazione dei costi dei servizi erogati
- fatturazioni di servizi non richiesti

Soggetti che si introducono abusivamente in sistemi informatici esterni al fine di procurare interesse o vantaggio alla Società. Es.:

- per conoscere un'offerta economica presentata per la partecipazione ad una gara d'appalto
- per conoscere il portafoglio clienti

Per la sicurezza la componente legale e quella tecnologica sono inscindibili

La Sicurezza delle informazioni è molto più che un problema tecnologico:

- Politiche;
- Procedure
- Processi organizzativi
- Riferimenti normativi: Codice Privacy ed i Provvedimenti dell'Autorità (in particolare Amministratori di Sistema), Circolare BI sulla vigilanza prudenziale, Codice Civile e Penale, D.Lgs. 231…
- Adempimenti contrattuali
- Attività di audit
- Attività di formazione

N.B. Il **Regolamento Informatico**, il **BYOD** e la riforma dell'art. **4 Statuto dei Lavoratori** sul controllo a distanza operata dal Jobs Act

Grazie!

Avv. Alessandro Cecchetti

acecchetti@consulentelegaleinformatico.it

https://it.linkedin.com/in/acecchetti

https://twitter.com/alececco84

Contatti

Sede legale e amministrativa:
Via Cividale, 51 – Montecatini Terme (PT) 51016
Tel. +39 0572 78166
Fax +39 0572 294540
Partita Iva e Codice Fiscale: 01651060475
Le nostre sedi: Montecatini Terme (PT), Roma, Milano
www.consulentelegaleinformatico.it

Per richieste progetti e preventivi:
info@consulentelegaleinformatico.it

Per organizzare eventi e corsi di formazione:
comunicazione@consulentelegaleinformatico.it

Seguici su: