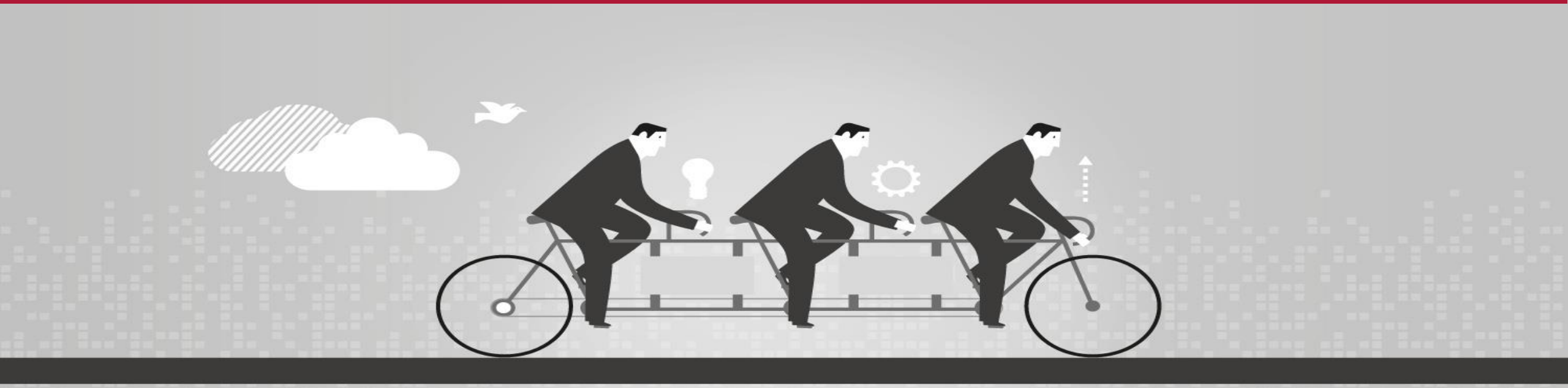
PRIVACY: COSA CAMBIA CON IL NUOVO REGOLAMENTO EUROPEO?



GABRIELE FAGGIOLI
DICEMBRE 2016

Evoluzione normativa

La storia

La normativa sulla privacy ha avuto una serie di passaggi rilevanti:

- **1996:** emanata la **prima legge sulla protezione dei dati personali** che prevedeva l'obbligo di adozione delle misure «minime» di sicurezze e delle misure di sicurezza «idonee». Fu una rivoluzione e per la prima volta i «dati personali» potevano essere trattati seguendo regole ben determinate con relative, importanti, responsabilità. Seguì poi le misure di sicurezza di cui al D.P.R. 28-07-1999, n. 318:
  - Pregio: grandissima valenza educativa
  - Difetto: ampiezza e ferraginosità della normativa

- **2003:** emanato il d.lgs 196/03 che ha completamente riaccorpato la normativa (e che è ancora la normativa in vigore). Le misure minime di sicurezza sono previste dall'Allegato B. Esistono però numerosi provvedimenti ancillari alla normativa che prevedono misure di sicurezza obbligatorie per una serie di trattamenti e interi settori di mercato
  - Pregio: plasmatura per settori di mercato
  - Difetto: scarsa capacità della norma di adeguarsi alle evoluzioni tecnologiche (cookies)

- **2018:** Regolamento UE. Il tema della sicurezza passa da una logica di «minimo» a una logica di «adeguato» in base ai rischi corsi (e nei casi previsti alla valutazione di impatto). In pratica ogni azienda o pubblica amministrazione deve analizzarsi e decidere come posizionarsi

Evoluzione normativa

- **Gli anni fra il 2011 e il 2016 sono stati caratterizzati da importanti novità nel settore normativo della sicurezza dei sistemi informativi con due linee di condotta contrapposte una di semplificazione e una di aggravamento:**
  - **Abolizione decreto Pisanu (semplificazione)**
  - **Provvedimento Garante per la protezione dei dati personali 12 maggio 2011 inerente la tracciabilità degli accessi ai dati bancari (aggravamento per mondo bancario)**
  - **Decreto legge n. 70/2011 "Semestre Europeo - Prime disposizioni urgenti per l'economia" successivamente convertito con legge n° 106/2011 (semplificazione)**
  - **Decreto Legge n. 201/2011, noto come Decreto Salva Italia, contenente le "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici", convertito con la legge del 22 dicembre 2011, n. 214 (semplificazione)**
  - **Decreto Semplificazioni 5/2012 approvato il 27.01.2012 convertito con la legge 4 aprile 2012 n. 35 (semplificazione)**
  - **Decreto Legislativo n. 69/2012 (aggravamento per settore telco)**
  - **Dec. Pres. Cons. 24.1.13 n° 67251 (infrastrutture critiche) (burocrazia e potenziale aggravamento)**
  - **Provvedimento del Garante sui cookies (4 maggio 2014)**
  - **Provvedimenti in materia di dossier sanitario e FSE (aggravamento)**
  - **Il nuovo articolo 4 della Legge 300/70**
  - **Etc….**
- **Ed ora: il nuovo Regolamento UE**

Linee di tendenza

Linee di tendenza normative

- Tendenza a porre in essere normative che impongono adempimenti mirati a proteggere l'azienda dall'interno. Solo in relazione alle infrastrutture critiche si tende a emanare normative che impongono misure di sicurezza a protezione di attacchi esterni
- Tendenza a porre in essere provvedimenti settoriali in sostituzione di provvedimenti generali
- Spinta alla sicurezza (obblighi di adottare misure di sicurezza) ma limiti alla sicurezza (tutela privacy del lavoratore e dei terzi)
- Estensione degli obblighi di raccogliere i log
- Estensione degli obblighi di segnalazione dei casi di data breach
- Regolamentazione del tempo di mantenimento dei dati
- Grande attenzione del tema security nell'ambito dei servizi IT e in particolare nel caso di servizi di cloud computing
- Creazione della figura del DPO

ITER LEGISLATIVO ORDINARIO UE

http://www.europarl.europa.eu/external/html/legislativeprocedure/default_it.htm

ITER LEGISLATIVO ORDINARIO UE

http://www.europarl.europa.eu/external/html/legislativeprocedure/default_it.htm

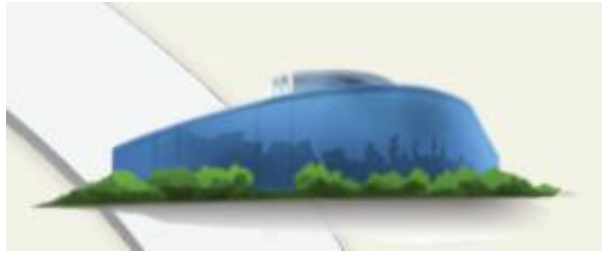
ITER LEGISLATIVO REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

25 gennaio 2012

Commissione europea presenta proposta di regolamento al Parlamento ed al Consiglio

14 marzo 2014

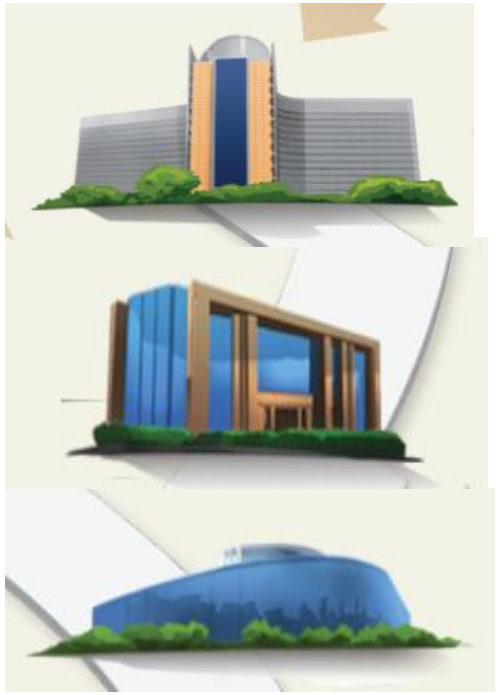
Parlamento presenta al Consiglio un testo emendato



11 giugno 2015

Consiglio adotta un orientamento generale

ITER LEGISLATIVO REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI



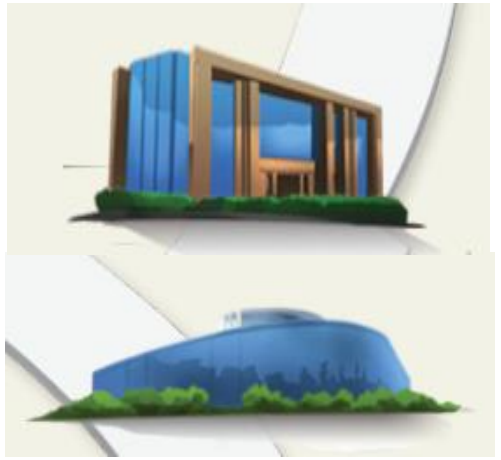
24 giugno 2015

Parlamento, Commisione e Consiglio avviano procedura di codecisione nota come “consultazione a tre” o “trilogo”

8 aprile 2016 (prima lettura Consiglio)
14 aprile 2016 (seconda lettura Parlamento)

4 maggio 2016

Pubblicazione in GUCE




24 maggio 2016 > 24 maggio 2018
25 maggio 2018
Regolamento 2016/679
IN VIGORE, NON APPLICABILE (?)
Direttiva 1995/46
IN VIGORE, DECADE il 24 maggio 2018
Direttiva 2002/58
NON DECADE ma dovrà essere riesaminata
Provvedimenti Autorità Garante
NON DECADONO fino a quando non verranno modificati, sostituiti, abrogati
Accordi internazionali su trasferimento dati
NON DECADONO fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissione UE
NON DECADONO fino a quando non verranno modificate, sostituite, abrogate

Responsabilità del titolare	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.
Responsabile della protezione dei dati	Figura indipendente nominata dal titolare e dal responsabile del trattamento. Svolge le seguenti funzioni: informare e consigliare il Titolare o il Responsabile in merito agli obblighi del Regolamento, verificarne l'applicazione e l'attuazione, fornire pareri, fungere da punto di contattato sia con gli interessati che con il Garante.
Registro dei trattamenti	Contenente i dati del/dei titolare/i e degli eventuali responsabili, le finalità del trattamento, una descrizione delle categorie di interessati e dei dati personali, i destinatari, gli eventuali trasferimenti verso Paesi terzi ed una descrizione generale delle misure di sicurezza. Tali documenti devono essere messi a disposizione del Garante e manutenuti sia dal titolare che dagli eventuali responsabili. I registri di cui sono tenuti in forma scritta.
Protezione sin dalla progettazione	Le misure a protezione di dati devono essere adottate già al momento della progettazione di un prodotto o software. Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire in ogni caso che siano trattati solo i dati necessari per ogni specifica finalità.

Responsabilità solidale di titolare e responsabile

Il Titolare e il Responsabile del trattamento sono responsabili in solido nei confronti dell'interessato, per un eventuale danno causato dal trattamento.

Responsabilità dei contitolari

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità.

Violazione di dati

Nel caso si verifichino violazioni di dati personali, il Titolare ne deve dare comunicazione all'Autorità di Controllo e, nei casi più gravi, anche agli interessati (attualmente ciò avviene solo per violazione di dati biometrici).

Designazione di terzi da parte del responsabile del trattamento

Nella nomina di un Responsabile del trattamento, il Titolare potrà prevedere una delega scritta specifica o generale per la designazione di eventuali Responsabili terzi, a fronte dell'obbligo di comunicare ogni nomina effettuata .

Eliminazione dell'obbligo di notifica	Viene eliminato l'obbligo generale di notificare all'autorità di controllo per il trattamento di dati personali, da sostituire con meccanismi e procedure efficaci che si concentrino piuttosto su quei trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche
Valutazione d'impatto	Sostituisce la notificazione. È la valutazione preliminare degli impatti a cui andrebbe incontro un processo qualora dovessero essere violate le misure di protezione dei dati. Necessita di alcune attività come la mappatura dei dati e dei trattamenti, la pianificazione degli interventi tecnologici e organizzativi di protezione dei dati con una valutazione complessiva di riduzione dello stato di rischio
Certificazioni	Richiesta volta ad ottenere il riconoscimento della conformità al Regolamento delle operazioni di trattamento dei dati.
Diritto all'oblio	Diritto di ottenere la cancellazione dei dati che lo riguardano purché non sussistano motivi legittimi per conservarli.
Limitazione del trattamento	L'interessato può richiedere la limitazione del trattamento qualora contesti l'esattezza dei dati nel periodo necessario al Titolare per verificare la correttezza, trattamento illecito, qualora i dati non siano più necessari al Titolare, ma l'interessato debba utilizzarli in sede giudiziaria, l'interessato si è opposto al trattamento in attesa di verifica.

Diritto alla portabilità dei dati

Possibilità per l'interessato di ricevere i propri dati personali in un formato strutturato, leggibile da dispositivo automatico e di uso comune. Introduce, inoltre, il diritto di ottenere, salvo impedimenti tecnici, la trasmissione diretta dei dati da un Titolare all'altro.

Nuove categorie di dati

Dati genetici, dati biometrici, dati relativi alla salute

Pseudonimizzazione

Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Trattamento e consenso per i minori di anni 16

Per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Grazie per l’attenzione!

gabriele.faggioli@p4i.it