REGOLAMENTO EUROPEO sulla DATA PROTECTION

Regolamento (UE) 2016/679

Stefano Carli

Vedi http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC

Che cosa è la **DATA PROTECTION?**

La data protection è il diritto di esercitare un controllo sulle informazioni che ci riguardano, evitando che vengano trattate abusandone.

Vedi http://www.dataprotection.org/web/guest/home/diritti/cosa-e-il-diritto-alla-protezione-dei-dati-personali

è un **DIRITTO**

- **DI MASSA**
- **DINAMICO**

I dati personali sono diventati la merce di scambio nella società tecnologica

Che cosa sono i

DATI PERSONALI?

Articolo 4
Definizioni

***«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*

A cosa servono i

Quanto valgono i 4

DATI PERSONALI?

- A formulare offerte mirate ai consumatori, per fidelizzarli ma anche per acquisirli
- A profilare e analizzare
- A migliorare l’efficacia dell’offerta

- Molto. Non fornire i propri dati spesso significa rinunciare a prodotti o servizi
- Molto. Perchè i dato personali sono la materia prima della società dell’informazione
- La protezione dei dati personali è un bilanciamento tra costi e benefici. A cosa siamo disposti a rinunciare per ottenerla?

Vedi anche: komando.com, The Guardian, adge.com

Le **TAPPE** della tutela dei dati personali

DIRETTIVA 95/46/CE

*Ha fissato i **principi generali** della normativa in materia di **dati personali** per consentire la **libera circolazione** dei dati personali in territorio europeo*

DIRETTIVE 2002/58/CE e 2009/136/UE

*Hanno introdotto alcune **precisazioni specifiche** rispetto alla Direttiva 95/46 che riguardano la raccolta di dati personali effettuata online e in particolare all'uso dei **cookies***

REGOLAMENTO (UE) 2016/679

*Nel 2012 la Commissione europea ha deciso di adottare un Regolamento per **abrogare** la direttiva 96/46. Non tutte le norme del Codice saranno abrogate. Rimarranno **inalterate** le norme attuative delle direttive 2002/58 e 2009/136.*

REGOLAMENTO EUROPEO

sulla
data protection

Dopo oltre quattro anni dalla proposta della Commissione, il 14 aprile 2016 il Parlamento europeo ha approvato in seconda lettura il Regolamento europeo concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei dati.

APPLICABILITÁ

Il Regolamento è entrato in vigore 20 giorni dopo la sua pubblicazione sulla Gazzetta ufficiale dell'Unione Europea e le sue disposizioni saranno **direttamente applicabili** in tutti gli stati membri nel 2018 (art. 99).

Non saranno necessarie leggi nazionali di recepimento come avviene per le direttive.

Il regolamento spinge fortemente per la **MINIMIZZAZIONE** del trattamento dei dati.

I nuovi imperativi da seguire sono due:

1 tratta **meno dati** che puoi

2 favorisci l' **anonimizzazione** e la **pseudonimizzazione**

Vedi art. 4, comma 5

A chi si applica la normativa?

Viene introdotto il principio dell'applicazione del diritto dell'Unione Europea **anche** ai trattamenti di dati personali **non** svolti nell'UE, se relativi all'offerta di beni e servizi a cittadini UE o tali da comportarne il monitoraggio dei loro comportamenti.

È una rivoluzione rispetto alla regola precedente in base alla quale la legge applicabile in caso di trattamento dei dati **è quella del luogo in cui ha sede il titolare del trattamento**, cioè il soggetto che raccoglie i dati, che definisce le modalità di raccolta (**territorialità**).

Articolo 3
Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Come dev'essere resa l'informativa?

L'informativa va resa in forma:

- **concisa**
- **trasparente**
- **intellegibile**
- con un linguaggio **semplice** e **chiaro**

Le informazioni sono fornite **per iscritto**.
Se richiesto dall'interessato possono essere fornite oralmente.

Se i dati non sono stati raccolti presso l'interessato deve essere indicata **l'origine** del dato.

Articolo 12
Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma **concisa**, **trasparente**, **intelligibile** e **facilmente accessibile**, con un **linguaggio semplice e chiaro**, in particolare nel caso di informazioni destinate specificamente ai **minori**. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Articolo 14
Informazioni da fornire qualora i dati personali **non** siano stati ottenuti **presso l'interessato**
[…]
2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
[…]
f) **la fonte da cui hanno origine i dati personali** e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

ICONA	INFORMAZIONI ESSENZIALI	SÌ/NO
	La **raccolta** di dati personali è limitata al minimo necessario per ogni specifica finalità del trattamento	
	La **memorizzazione** di dati personali è limitata al minimo necessario per ogni specifica finalità del trattamento	
	Il **trattamento** di dati personali è limitato alle finalità per le quali sono stati raccolti	
	Non sono **forniti** dati personali a terze parti commerciali	
	Non sono effettuati **la vendita o l'affitto** di dati personali	
	I dati personali non sono memorizzati in forma **non cifrata**	

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data is **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data is **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data is **processed** for purposes other than the purpose it was provided for	
	No personal data is **disseminated** to private third parties for purposes other than the purpose it was provided for	
	No personal data is **sold**	
	No personal data is retained in **unencrypted** form	

Come cambia il consenso?

il

consenso

DEVE ESSERE

libero
specifico
informato
inequivocabile

Non è più richiesto il requisito del **consenso espresso** se non per attività di **profilazione**.

Sono in ogni caso illegittimi i consensi raccolti con caselle prebarrate.

Articolo 4
Definizioni
[…]
11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà **libera**, **specifica**, **informata** e **inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o **azione positiva inequivocabile**, che i dati personali che lo riguardano siano oggetto di trattamento;

Abolizione della notificazione

Tale adempimento è considerato dal Legislatore un obbligo che comporta **oneri** amministrativi e finanziari **senza** aver mai veramente contribuito a migliorare la protezione dei dati personali.

Viene quindi **abolito** l'obbligo generale di notificazione e **sostituirlo con meccanismi e procedure efficaci** che si concentrino piuttosto su quelle operazioni di trattamento che potenzialmente presentano **rischi specifici** per i diritti e le libertà degli interessati.

In tali casi sarà necessaria una **valutazione d'impatto** sulla protezione dei dati, da effettuarsi **prima** del trattamento.

Vedi (90) e art. 35

considerando quanto segue:
[…]
(89) La direttiva 95/46/CE ha introdotto un **obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali**. Mentre tale obbligo comporta **oneri** amministrativi e finanziari, **non ha sempre contribuito** a migliorare la protezione dei dati personali. È pertanto opportuno **abolire** tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Privacy Impact Assessment

I Titolari dovranno effettuare una **Valutazione degli impatti privacy** **(Data Protection Impact Analysis – DPIA o PIA)** fin **dal momento della progettazione** del processo aziendale e degli applicativi informatici di supporto nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti **rischi specifici** per i diritti e le libertà degli interessati.

- Analisi dei rischi
- Definire i gap rispetto alla corretta gestione dei rischi
- Stabilire un piano d'azione per colmare i gap
- Controllare periodicamente gli interventi effettuati per mitigare i rischi

Es. Trattamenti quali: la valutazione **sistematica** di aspetti della personalità dell'interessato o quelli volti ad analizzarne la situazione **economica**, **l'ubicazione**, lo stato di **salute**, **l'affidabilità** o il **comportamento**, mediante un trattamento automatizzato; per trattamenti di dati concernenti la vita **sessuale**, la prestazione di servizi **sanitari**, lo stato di salute, la **razza** e **l'origine etnica**; o, ancora, per trattamenti di dati in archivi su larga scala riguardanti minori, dati genetici o dati biometrici

Vedi art. 35 comma 3

Articolo 35
Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, **può presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una **valutazione dell'impatto dei trattamenti previsti** sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 **è richiesta in particolare nei casi seguenti**:
[…]

Data protection officer

Viene introdotta la figura del "Responsabile per la protezione dei dati" o Data protection officer (DPO). Non è un responsabile del trattamento: è il "manager" del trattamento dei dati

PER CHI È OBBLIGATORIO?

- Tutte le autorità e organismi pubblici
- Le imprese che trattino i dati di un rilevante numero di persone o tipologie che, per natura, oggetto o finalità sono definite "a rischio" dalla normativa.

CHI È?

- Designato come soggetto referente del Garante
- Gode di ampia autonomia
- Deve possedere competenza professionale
- Può essere un soggetto esterno
- Il suo mandato dura quattro anni ed è rinnovabile e revocabile

COSA FA?

- **sensibilizzare** e **consigliare** il Titolare in merito **agli obblighi** (misure e procedure tecniche e organizzative) derivanti Regolamento;
- **sorvegliare** l'applicazione delle **politiche** compresa l'attribuzione delle responsabilità, la **formazione** del personale che partecipa ai trattamenti e **l'effettuazione** degli **audit** connessi;
- **sorvegliare** l'applicazione del **Regolamento**, con particolare riguardo alla protezione fin dalla progettazione, alla protezione di default, alla sicurezza dei dati, alle informazioni dell'interessato ed alle richieste degli stessi per esercitare i diritti riconosciuti;
- controllare che il Titolare effettui la Valutazione d'impatto sulla protezione dei dati (c.d. **DPIA o PIA**) e richieda all'Autorità di Controllo l'autorizzazione preventiva o la consultazione preventiva nei casi previsti;
- fungere da **punto di contatto** per l'Autorità di Controllo per questioni connesse al trattamento e consultarla, se del caso, di propria iniziativa;
- **informare** i rappresentanti del personale (es. rappresentanti sindacali) sui trattamenti che riguardano i dipendenti.

Dovere di documentazione

Sarà necessario elaborare un **sistema documentale** di gestione della privacy contenente **tutti gli atti**, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento.

È l'applicazione operativa del principio di rendicontazione (o di "**accountability**")

Principio secondo cui il Titolare del trattamento deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi - una serie "nutrita" di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento.
Tutte le operazioni di trattamento devono essere tacciabili e verificabili.

Articolo 30
Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
[…]

Privacy by design

Mettere in atto meccanismi per garantire che siano trattati - di default - solo i dati personali necessari per ciascuna finalità specifica del trattamento

Privacy by default

I titolari del trattamento dovranno prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati.

Articolo 25
Protezione dei dati **fin dalla progettazione** e protezione per **impostazione predefinita**

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al **momento di determinare** i mezzi del trattamento sia all'atto del **trattamento stesso** il titolare del trattamento mette in atto misure tecniche e **organizzative adeguate**, quali la **pseudonimizzazione**, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Violazione dei dati personali

Data breach: La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Vedi art. 4 comma 12

In caso di data breach i titolari del trattamento, pena sanzioni, dovranno mettere in atto **due** azioni

- La notificazione della violazione all'autorità di controllo entro 72 ore dal fatto
- La segnalazione al diretto interessato (senza ritardo ingiustificato)

Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
[…]

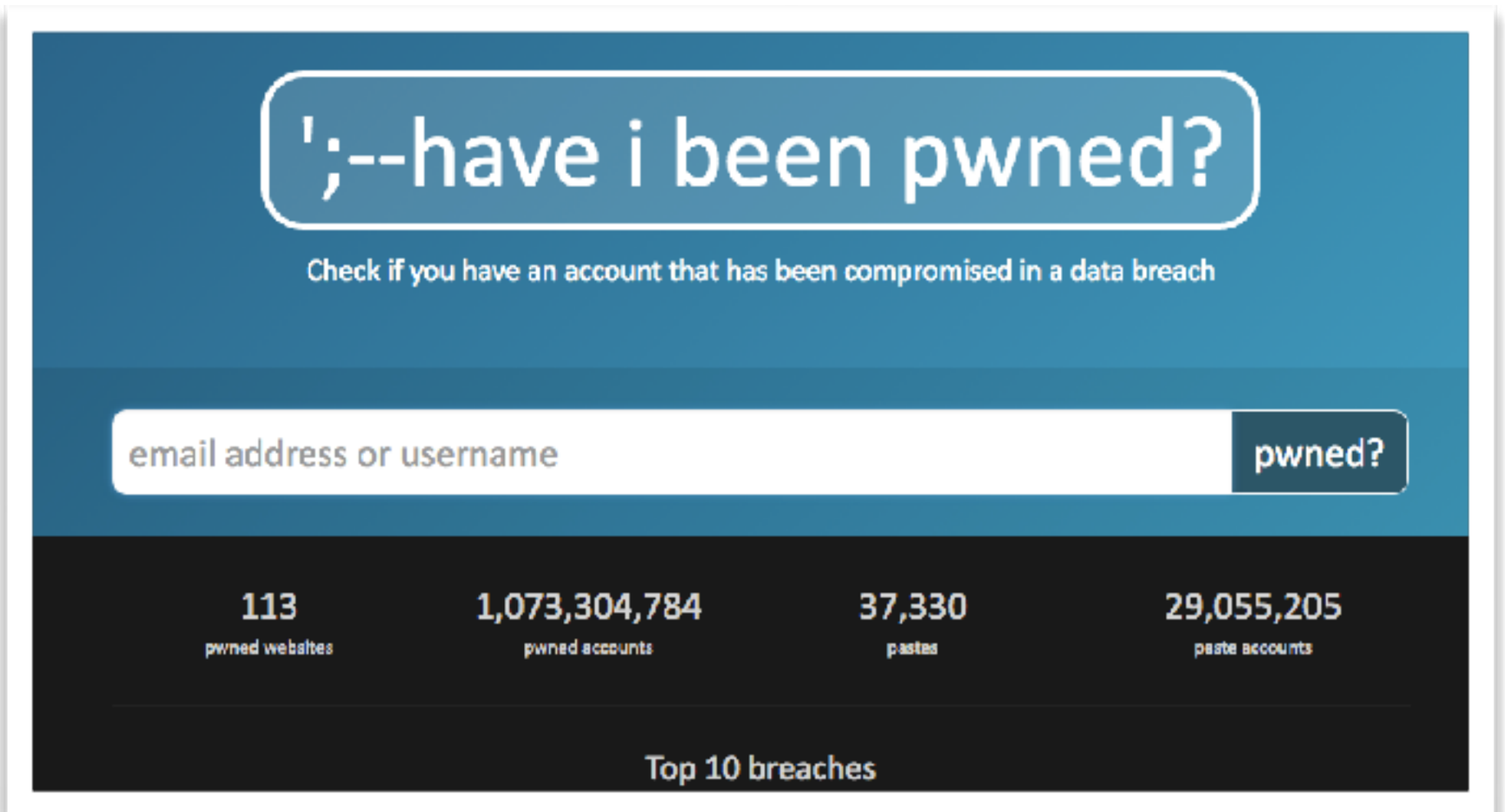
il tuo account
ha subito
DATA BREACH?

il suo si!

http://www.lastampa.it/2016/06/06/tecnologia/zuckerberg-colpito-dagli-hacker-rubati-account-twitter-e-pinterest-RCy1CgmjJZV3i99wEzvL1O/pagina.html

il tuo indirizzo email
ha subito
DATA BREACH?

Puoi scoprirlo su
https://haveibeenpwned.com/



Diventano molto pesanti le **SANZIONI**

fino a
20.00.000 €

o fino al
4% del fatturato mondiale totale annuo *dell'esercizio precedente, se superiore*

Vedi art. 83 comma 4, 5 e 6

Diventano molto pesanti le **SANZIONI**

Le sanzioni e parte della normativa sono pensate per incidere sui comportamenti dei grandi gruppi multinazionali che trattano dati in diverse aree geografiche e spesso cercano di individuare i “paradisi legali” riguardo al trattamento dei dati personali per eludere norme e criteri di comportamento definiti dalle nazioni più “rigorose”.