TÜV SÜD Italia

Scegli la certezza.
Aggiungi valore.

IL NUOVO REGOLAMENTO PRIVACY

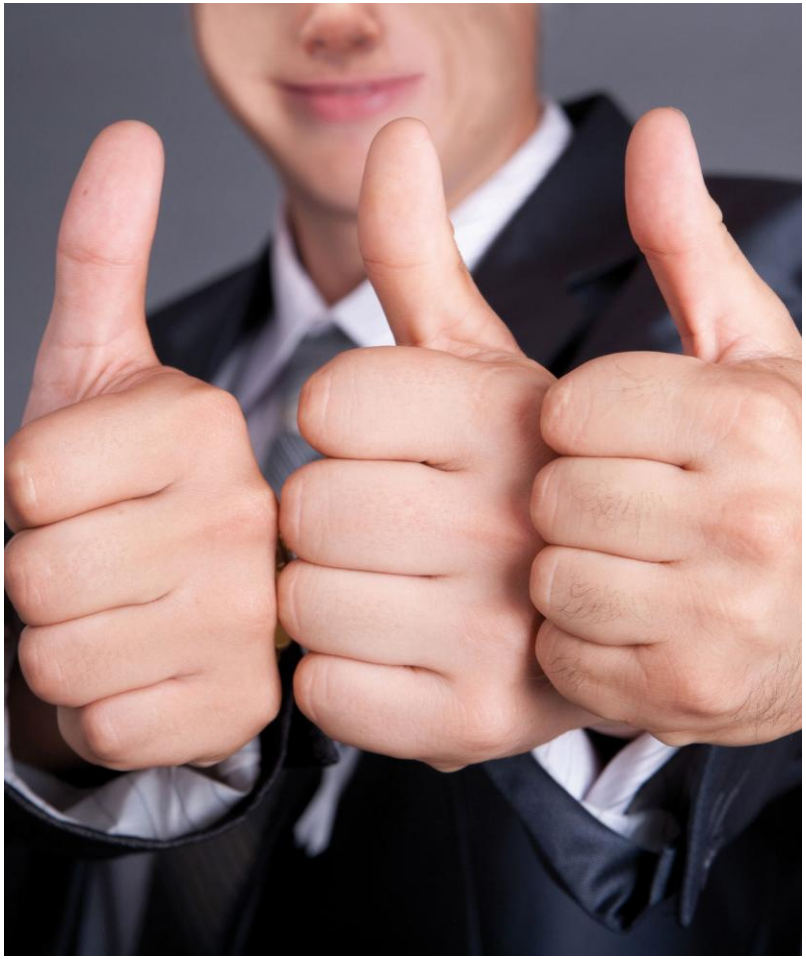
TÜV ITALIA
Management Services Division

Sabrina Bruschi

06 SETTEMBRE 2017
Bologna

Inquadramento

Il Regolamento Europeo UE 2016-679: Primi dati



- Pubblicazione del Regolamento sulla Gazzetta Ufficiale L119 dell'Unione Europea del Parlamento Europeo e del Consiglio il 04/05/2016 a fronte dell'approvazione del 27/04/2016

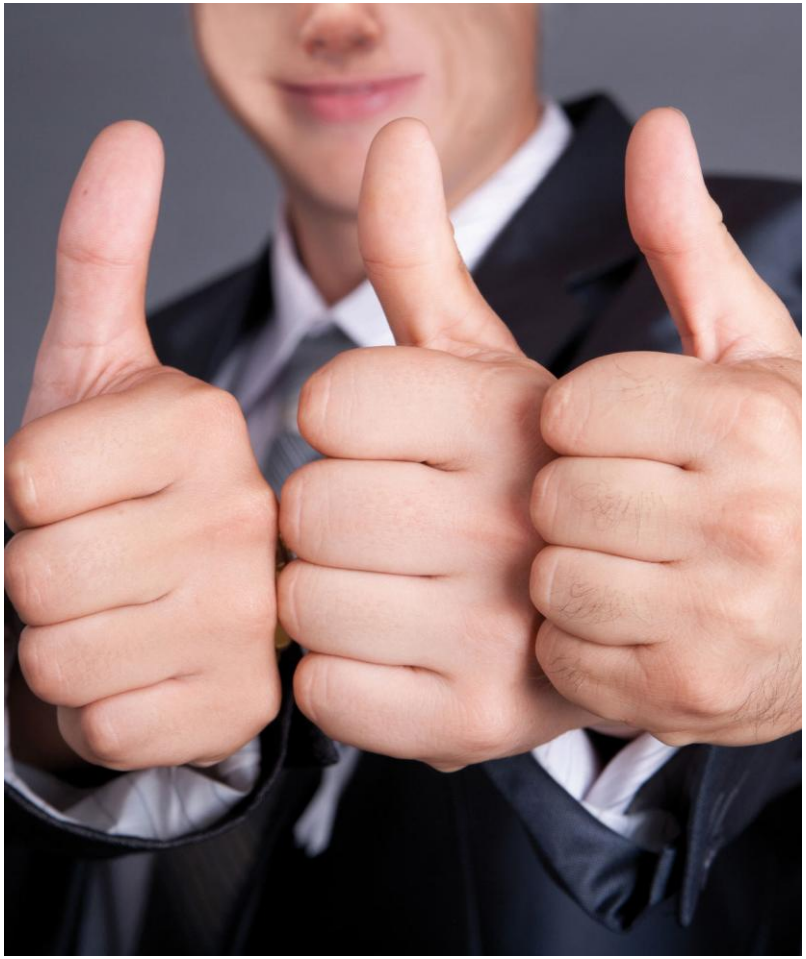
- E' relativo alla: "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"

- Diventerà applicabile in tutti i paesi dell'Unione Europea a partire dal 25 maggio 2018, data in cui dovrà essere garantito il perfetto allineamento fra normativa nazionale e quella Europea (Recepimento)

- Armonizza la normativa della privacy in tutti i paesi dell'Unione Europea

Inquadramento

Il contesto da cui nasce



- La **Direttiva 95/46/CE** rappresenta l'atto normativo di riferimento in materia di protezione dei dati personali all'interno dell'Unione Europea (cd. Direttiva Madre)

- Il **D.lgs. 30 giugno 2003, n. 196, Codice per la Protezione dei dati personali, è il testo normativo che razionalizza, semplifica e coordina, in un Testo Unico di riferimento, tutte le disposizioni legislative e regolamentari in materia di Privacy e Protezione dei Dati Personali, assorbendo la L. 31 dicembre 1996, n. 675, con cui si era data attuazione alla Direttiva Madre**

- Il Regolamento è composto da 173 "Considerando" e 99 articoli, è entrato in vigore il 24 maggio 2016, ma sarà efficace e direttamente applicabile a partire dal 25 maggio del 2018

Le novità introdotte dal Regolamento

Dato personale

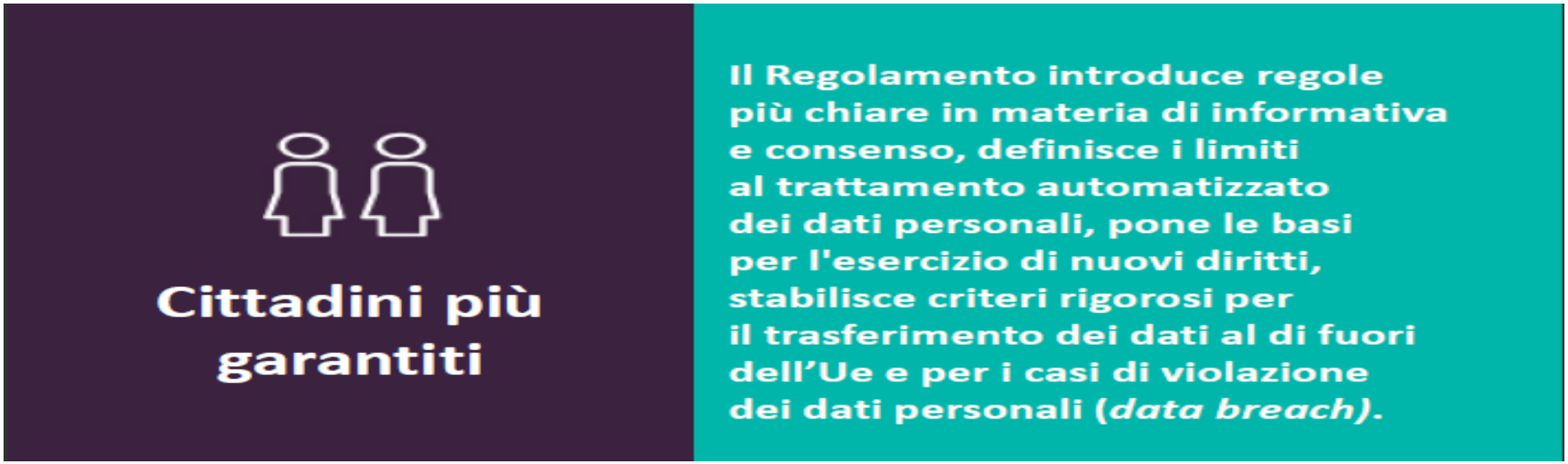
Qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate direttamente o indirettamente anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo.

Sono, ad esempio, dati personali: il nome e cognome o denominazione; indirizzo, il codice fiscale; cioè tutti quegli elementi caratteristici della sua identità FISICA, FISIOLOGICA, GENETICA, PSICHICA, ECONOMICA, CULTURALE E SOCIALE

Fonte: www.garanteprivacy.it

Inquadramento: i presupposti del gruppo di lavoro europeo

Le novità introdotte dal Regolamento



Violazione dei dati personali

Violazione di SICUREZZA che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, memorizzati o comunque trattati.

Le novità introdotte dal Regolamento: I DIRITTI

Diritto all'Oblio (Artt. 65 e 66)

Il Regolamento codifica il diritto dell'interessato di chiedere ai motori di ricerca di deindicizzare una pagina web o chiedere ad un sito web di cancellare informazioni

Portabilità dei dati (artt. 13 e 20)

All'interessato viene riconosciuto il diritto di ottenere la restituzione dei propri dati personali trasmessi ad un'azienda o ad un servizio on-line e trasmetterli ad altri (social network fornitori di servizi internet, fornitori di streaming on-line etc…)

Le novità introdotte dal Regolamento: I DOVERI

Data Breach Notification (artt. 33 e 34)

La violazione dei dati personali va comunicata appena si viene a conoscenza di un'avvenuta violazione dei dati personali trattati.

Il Titolare del trattamento deve notificare la violazione dei dati al Garante (senza ingiustificato ritardo) entro 72 ore dal momento in cui è venuto a conoscenza del fatto.

Trascorso le 72 ore la notifica necessita delle motivazioni del ritardo nella comunicazione.

Le novità introdotte dal Regolamento: I DIRITTI

Informativa

L'interessato ha diritto ad essere informato dell'esistenza del trattamento e delle sue finalità e delle ulteriore circostanze necessarie alla sua tutela.

Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa.

IL CONSENSO DEVE ESSERE **INEQUIVOCABILE!!!** (ART. 32)

Consenso dell'interessato

Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo steso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile che i dati personali che lo riguardano siano oggetto di trattamento

Il consenso deve essere **POSITIVO** ed **UNICO**

Le novità introdotte dal Regolamento: I DIRITTI

Trattamento Automatizzato detta "Profilazione"
Il Regolamento sancisce il diritto a non subire profilazioni (trattamenti automatizzati) inconsapevoli.

Sportello Unico
L'interessato può rivolgersi all'autorità di protezione dei dati del proprio paese per segnalare eventuali violazioni, qualunque sia il luogo in cui il trattamento è effettuato.

Le novità introdotte dal Regolamento: I principi

Principio di Accountability

Il principio di responsabilizzazione significa che si chiede al titolare del trattamento di mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. Aiutano a dimostrare la conformità al regolamento l'adesione ai codici di condotta o ad un meccanismo di certificazione.

Il principio di accountability coinvolge sia il titolare che il responsabile del trattamento.

Le novità introdotte dal Regolamento: I DIRITTI

Cosa significa Privacy by design?
Significa protezione dei dati fin dalla progettazione. Significa ridurre al minimo il trattamento dei dati personali mediante misure (tecniche ed organizzative) quali, ad esempio, la pseudonimizzazione dei dati personali.

Per pseudonimizzazione si intende il trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche ed organizzative intese a garantire che tali dati personali non siano attribuiti ad una persona identificata od identificabile.

Le novità introdotte dal Regolamento: I DIRITTI

Cosa significa Privacy by default?

Significa che la tutela della protezione del dato deve diventare l'impostazione predefinita. Il titolare del trattamento infatti deve adottare misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Il ruolo Responsabile della protezione dei Dati (DPO – art. 37)

Il Regolamento UE 2016/679 introduce una **nuova figura** chiamat[illegible]a **Protection Officer (DPO)** e la sua nomina è obbligatoria p[illegible]blici e facoltativa per i soggetti privati ad eccezione di alcu[illegible]ati a rischio e fatto salvo da una diversa disposizione legi[illegible]

Linee-Guida sui responsabili della protezione dei dati – WP243
Adottate dal gruppo di lavoro Art. 29 il 13 dicembre 2016

I suoi compiti sono quelli di:

- informare e fornire **consul[illegible]l trattamento o al responsabile del trattamento d[illegible]**to agli obblighi che derivano dal Regolam[illegible]
- v[illegible]**ione ed attuazione del Regolamento UE 2016/679** e di [illegible]mpimenti ad esso collegati
- [illegible]re un **parere in merito alla valutazione d'impatto sulla protezione dei dati** e sorvegliarne lo svolgimento
- **cooperare ed interloquire** con l'Autorità Garante

Quando è necessario il Responsabile della protezione dei dati?

Devono designare obbligatoriamente un Responsabile della protezione dei dati (DPO):

a) **amministrazioni ed enti pubblici**, fatta eccezione per le autorità giudiziarie;
b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati;
c) tutti i soggetti la cui attività principale consiste nel trattamento, su **larga scala**, di **dati personali particolare** (vedi art. 9), relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Un titolare del trattamento o un responsabile del trattamento possono comunque designare un DPO (Responsabile della protezione dei dati) anche in casi diversi da quelli sopra indicati.
Un gruppo di imprese o soggetti pubblici possono nominare un unico esponsabile della protezione dei dati.

Ruoli

Che caratteristiche deve avere

Il soggetto che viene designato come "Responsabile della protezione dei dati" (DPO), deve:

- possedere un'**adeguata conoscenza della normativa e** delle prassi di gestione dei dati personali nazionali ed europee (art.37, par.5)
- adempiere alle sue funzioni in **piena indipendenza ed in assenza di conflitti di interesse (art.38, par.6)**
- operare **alle dipendenze del titolare oppure sulla base di un contratto di servizio (art.37, par.6)**

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le **risorse umane e finanziarie necessarie all'adempimento dei suoi compiti (art.38, par.2)**

La violazione dei dati personali

Il Nuovo Regolamento Europeo introduce per la prima volta l'obbligo della **Data Breach Notification**, notifica in caso di violazioni di dati.

La **violazione di dati personali** (data breach) è definita come:

«violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico nella Comunità»

La violazione dei dati personali

Quando la violazione comporta un rischio elevato per i diritti e le libertà dei soggetti interessati, la violazione deve essere comunicata **a ciascun soggetto coinvolto** individualmente o, laddove una comunicazione individuale richieda sforzi sproporzionati, tramite una comunicazione pubblica.

Livello di rischio	Effetti	Azioni previste
Trascurabile	Nessun pregiudizio per il cliente oggetto di valutazione	Nessuna comunicazione prevista
Basso	Nessun pregiudizio significativo per il cliente oggetto di valutazione	Prevista comunicazione al Garante della Privacy
Medio	Possibilità di pregiudizio per i clienti oggetto della violazione	Prevista comunicazione al Garante della Privacy ed al cliente oggetto della violazione
Alto	Possibilità di un significativo pregiudizio per i clienti oggetto della violazione	Prevista comunicazione al Garante della Privacy ed al cliente oggetto della violazione
Molto alto	Possibilità di grave pregiudizio per il cliente	Prevista comunicazione al Garante della Privacy ed al cliente oggetto della violazione

La violazione dei dati personali

La notificazione prevista dal nuovo regolamento dovrà contenere **indicazioni sulla natura della violazione dei dati personali, le probabili conseguenze e le misure adottate per porre rimedio alla violazione.**

La nuova normativa, oltre a contemplare un notevole inasprimento delle sanzioni (fino a un massimo di **20.000.000 di euro o al 4% del fatturato mondiale annuo**), prevede anche un cambio di paradigma nella logica della protezione dei dati personali.
Si passa dall'obbligo di applicazione (almeno) delle misure minime di sicurezza contenute nell'allegato B al D.Lgs. 196/03, a un più generale obbligo di responsabilizzazione del Titolare (c.d. **accountability**)

Parliamo di Codici di Condotta e Certificatione

NOVITA ASSOLUTA!!!!!

Questa è un'importante novità nel regolamento.
L'obiettivo è di creare una trasparenza tale da permettere agli interessati di valutare il livello di protezione dei dati dei relativi prodotti e servizi dimostrando il rispetto del regolamento.
L'adozione di Codici di condotta, e di certificazioni è volontaria ed ha lo scopo di dimostrare la conformità della propria gestione Privacy.

AMBITI DI INTERVENTO

D.LGS 231 / ANTI-BRIBERY

VALUE CHAIN

BUSINESS CONTINUITY

CSR

CYBER SECURITY

HSE

PRIVACY

Italia

Scegli la certezza.
Aggiungi valore.

Grazie per la vostra attenzione

Sabrina Bruschi
Cell. 3487224187
Sabrina.bruschi@tuv.it

Se interessato, visita il nostro sito www.tuv.it e iscriviti alla Newsletter TÜV Italia. Sarai sempre aggiornato sulle nostre iniziative!