Regolamento UE 2016/679 in materia di protezione dei dati personali

-

GENERAL DATA PROTECTION REGULATION

LO SCENARIO DOPO IL 25 MAGGIO 2018: MA PRIMA?

AVV. FILIPPO CAMPAGNOLI

SLR STUDI LEGALI RIUNITI

PERCHÈ UN GENERAL DATA PROTECTION REGULATION ?

Nel maggio 2016 l'Europa ha concluso un percorso normativo per la redazione del GDPR durato quasi un quinquennio, il più lungo della storia legislativa delle comunità europee e dell'Unione europea.

Questa lunga gestazione è stata frutto della più intensa e vivace attività di lobbying che si sia mai stata registrata a Bruxelles ed a Strasburgo.

La prima bozza di GDPR è stata formulata nel gennaio del 2012, a cui sono seguiti oltre 4mila emendamenti al Parlamento UE, attraversando un burrascoso iter legislativo caratterizzato da un acceso dibattito politico e forti pressioni da parte delle lobby americane dei colossi di internet, giungendo dopo oltre quattro anni ad un compromesso durante i negoziati finali nel dicembre 2015, per essere poi pubblicato sulla Gazzetta Ufficiale dell'Unione Europea a maggio del 2016

PERCHÈ UN GENERAL DATA PROTECTION REGULATION ?

Perché l'Unione Europea ha deciso di adottare il nuovo Regolamento meglio noto con il nome di **GENERAL DATA PROTECTION REGULATION** (C.D. **GDPR**)?

PERCHÈ UN GENERAL DATA PROTECTION REGULATION ?

1. MAGGIORE PRODUZIONE E UTILIZZO DI DATI (PERSONALI)

Negli ultimi anni si sta realizzando una rivoluzione che si fonda sui dati (personali e non), sul loro possesso, sulla liceità del loro trattamento, sulla loro comunicazione e sul profitto che ne deriva.

Nel 2015 sono state prodotte più informazioni di quante ne fossero state create in tutti gli anni precedenti della civiltà umana

Ad una **maggiore produzione** di dati si accompagna una **maggiore velocità** ed ambito di **diffusione**: la navigazione in internet, i social network, le applicazione negli smartphone hanno condotto all'aumento di soggetti ed oggetti (IOT) connessi fra loro.

Scarsa consapevolezza dei dati forniti e del **valore** degli stessi da parte degli interessati.

PERCHÈ UN GENERAL DATA PROTECTION REGULATION ?

2. DIGITAL SINGLE MARKET - MERCATO UNICO DIGITALE

A livello comunitario è risultata sempre più pressante l'esigenza di aggiornare ed armonizzare le norme dei singoli stati europei anche al fine di creare il MERCATO UNICO DIGITALE, ossia un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi, dei capitali e dei **dati**:

NECESSITÀ DI UN LIVELLO ELEVATO DI PROTEZIONE DEI CONSUMATORI E DEI DATI PERSONALI CON REGOLE COMUNI

PERCHÈ UN GENERAL DATA PROTECTION REGULATION ?

1. **Le DIRETTIVE COMUNITARIE**
   - 95/46/CE cd Direttiva Madre in materia di tutela dei dati personali
   - 2002/58/CE direttiva relativa alla vita privata e alle comunicazioni elettroniche
   - 2009/136/UE direttiva in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche
   - 2009/140/CE direttiva in materia di reti e servizi di comunicazione elettronica.
   - 2016/1148/UE c.d. Direttiva NIS: misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione.

2. **Il CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - DLgs n. 196/2003**

3. **PROVVEDIMENTI DEL GARANTE ITALIANO** (DISMISSIONE DELLA SPAZZATURA ELETTRONICA - c.d RAEE – 2008, AMMINISTRATORI DI SISTEMA – 2008, VIDEOSORVEGLIANZA – 2010, COOKIE – 2014, BIOMETRIA – 2014)

3. BIG DATA

Necessità di protezione dei c.d. «**big data**», ovvero grandi volumi di dati che vengono trattati e trasferiti in paesi terzi con legislazioni differenti rispetto a quelle europee.

RILEVANTE VALORE COMMERCIALE DEI DATI PERSONALI: in particolare la concentrazione di informazioni nelle mani di pochi soggetti in grado di disporre di algoritmi software e apparecchiature hardware in grado di gestire e trattare una quantità di informazioni illimitate per scopi di diversa natura.

L'utilizzo e la gestione di queste informazioni, processate da sistemi informatici, comporterà effetti di alterazione nel modo di produrre e scambiare beni, consentirà di profilare miliardi di persone in tempo reale e di prevedere i loro comportamenti e massificarne l'indirizzo.

4. ECONOMIA DIGITALE – INDUSTRIA 4.0

L'economia globale diventa digitale: le tecnologie dell'informazione e della comunicazione non costituiscono più un settore a sé stante, bensì il fondamento stesso di tutti i sistemi economici innovativi moderni.

Si afferma un nuovo paradigma industriale – è la quarta rivoluzione denominata **Industria 4.0** – in cui tutte le fasi produttive sono gestite e condizionate dalle informazioni raccolte **dalla progettazione sino al post-vendita** da eterogenee tecnologie abilitanti digitali che interconnettono sistemi produttivi, prodotti e consumatori.

Ex: NETFLIX ha ideato e prodotto una serie televisiva (House of Cards) i cui contenuti sono stati integralmente tratti dall'analisi del comportamento dei fruitori sulla propria piattaforma.

PERCHÈ UN GENERAL DATA PROTECTION REGULATION ?

5. CRESCE L'INDUSTRIA DEL CYBERCRIME

- +8,35% di attacchi informatici gravi a livello globale rispetto al semestre precedente
- Aumentano del 253% gli attacchi verso "bersagli multipli indifferenziati" condotti da un'unica forza criminale, secondo una logica "industriale"
- L'Europa è l'unico continente dove cresce la percentuale di vittime
- Utilizzati soprattutto Malware (+86%, di cui oltre un terzo Ransomware) e tecniche di
- Phishing/Social Engineering (+85%)
- Gli smartphone nel mirino: sempre più diffusi malware specifici per tutte le piattaforme

I dati relativi al primo semestre 2017 sono stati 571 gli attacchi gravi di dominio pubblico (ovvero attacchi che hanno avuto un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili), che corrispondono ad una crescita dell'8,35% rispetto al secondo semestre 2016.

Gli autori del Rapporto Clusit evidenziano che il primo semestre 2017 è stato il peggiore di sempre, confermando una inesorabile tendenza ascendente dal 2011 ad oggi.

6. PRIVACY: DA DIRITTO ALLA RISERVATEZZA A DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

L'istituto nasce come diritto "**a essere lasciato solo**" (*to be let alone*) negli Stati Uniti nel 1890, e viene elaborato nel nostro paese a partire dagli anni '60-'70 come generico diritto alla libera determinazione nello svolgimento della propria personalità.

Privacy è il:

- **diritto alla non intromissione nella sfera privata da parte di terzi**.
- **diritto di controllo su qualsiasi informazione riguardante una persona che ne consenta l'identificazione diretta o indiretta**

7. NECESSITA' DI NUOVO APPROCCIO ALLA TUTELA DEI DATI

Necessità di creare uno strumento che sia al passo con i tempi.

Approccio basato sul rischio e sull'**accountability** (**responsabilizzazione**): la valutazione del rischio nel trattamento dei dati è effettuata dal titolare e dal responsabile e l'intervento delle Autorità è solo successivo ed eventuale, superando il precedente concetto di norme (cd misure minime) a cui il Titolare del trattamento doveva adeguarsi.

GENERAL DATA PROTECTION REGULATION

LA GESTIONE DEI DATI PERSONALI NON È PIÙ SOLO UN **ADEMPIMENTO,** MA DIVENTA UN **PROCESSO AZIENDALE** CHE INCIDE SULL'**ORGANIZZAZIONE DELLE IMPRESE.**

GDPR, General Data Protection Regulation, è la regola generale con cui l'Unione Europea ha scelto di **potenziare ed omogeneizzare** la protezione dei dati personali dei cittadini dell'Unione, così come dei residenti nella stessa, sia all'interno dei confini, sia al di fuori.

GENERAL DATA PROTECTION REGULATION

Entro il **25/05/2018** tutte le imprese dovranno adeguarsi al regolamento UE n. 2016/679 concernente la privacy direttamente applicabile in ciascun stato membro.

IL GDPR non abroga il Codice Privacy (Dlgs. 196/2003) che, in assenza di legge nazionale di abrogazione e armonizzazione, resterà in vigore anche dopo il 25 maggio 2018 e questo creerà problemi interpretativi se e quando potrà essere applicato il codice italiano o quando dovrà essere applicato il Regolamento.

STRUTTURA DEL GDPR

172 CONSIDERANDO e 99 ARTICOLI

CAPO I – **DISPOSIZIONI GENERALI**

CAPO II – **PRINCIPI**

CAPO III – **DIRITTI DELL'INTERESSATO**

CAPO IV – **TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO**

CAPO V – **TRASFERIMENTI DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI**

CAPO VI – **AUTORITA' DI CONTROLLO INDIPENDENTI**

CAPO VII – **COOPERAZIONE E COERENZA**

CAPO VIII – **MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI**

CAPO IX – **DISPOSIZIONI RELATIVE A SPECIFICHE SITUAZIONI DI TRATTAMENTO**

CAPO X – **ATTI DELEGATI ED ATTI DI ESECUZIONE**

CAPO XI – **DISPOSIZIONI FINALI**

DATO PERSONALE:

Sono dati personali le informazioni che identificano o rendono identificabile una **persona fisica** e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc….
Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (ex n. cellulare, n. IP, ….) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

DATI IDENTIFICATIVI

- nome e cognome
- indirizzo di casa
- indirizzo email
- Codice fiscale
- numero di passaporto
- indirizzo IP
- numero di targa del veicolo
- numero di patente
- numeri di carta di credito
- data di nascita
- luogo di nascita
- numero di telefono
- account name o nickname.

…..

DATI SOGGETTI A TRATTAMENTO SPECIALE (EX DATI SENSIBILI)

L'articolo 9 del GDPR sancisce un trattamento speciale per i dati che rivelino:

- l’origine razziale o etnica
- le opinioni politiche
- le convinzioni religiose o filosofiche, o l’appartenenza sindacale
- dati genetici
- dati biometrici intesi a identificare in modo univoco una persona fisica
- dati relativi alla salute (anche la semplice ferita ad una mano) o alla vita sessuale o all’orientamento sessuale della persona

TRATTAMENTO

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

PRINCIPI DEL TRATTAMENTO DEI DATI

1. **Liceità** dei dati in possesso, ovvero i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, ossia in conseguenza di una idonea base giuridica (consenso, adempimento contratto, adempimento norme di legge …..)
2. **Limitatezza delle finalità**, quindi i dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
3. **Minimizzazione**, i dati raccolti devono essere pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **Esattezza**, ossia, i dati personali raccolti saranno 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;
5. **Limitazione della conservazione**, quindi i dati dovranno essere 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. Tale periodo deve essere inserito nell'informativa.
6. **Sicurezza dei dati personali**, cioè 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.

INFORMATIVA

L'art. 13 del GDPR elenca in modo puntuale quanto il titolare deve sempre indicare in un'informativa:

- La **base giuridica** del trattamento
- Se **trasferisce** i dati personali in Paesi terzi
- Il **periodo** di conservazione dei dati o i criteri seguiti per stabilire tale periodo
- I contatti del **DPO** (se presente)
- Il diritto di presentare un **reclamo** all'autorità di controllo
- Se il trattamento comporta **processi decisionali automatizzati**

INFORMATIVA

IL REGOLAMENTO SPECIFICA QUALI DEBBANO ESSERE LE CARATTERISTICHE DELL'INFORMATIVA:

- Deve avere forma **concisa, trasparente, comprensibile** per l'interessato e **facilmente accessibile**
- Deve essere **scritta in un linguaggio chiaro e semplice**
- Viene consegnata in forma prevalentemente **scritta e in formato elettronico** (sono comunque ammessi altri mezzi)
- Sono ammesse **icone** per la sua composizione, purché queste siano accompagnate da una informativa estesa (queste icone dovranno essere uguali in tutta Europa e saranno definite dalla Commissione Europea)

Per quanto riguarda l'esonero dall'informativa, il Regolamento sottolinea che spetta al Titolare del Trattamento valutare se questa rappresenti uno sforzo sproporzionato.

LE NOVITÀ SUL CONSENSO AL TRATTAMENTO:

Il consenso (uno delle *basi giuridiche* per cui è lecito il trattamento) deve essere:

- libero, specifico, informato e inequivocabile (non è ammesso infatti il consenso tacito o presunto)
- manifestato attraverso "**dichiarazione o azione positiva inequivocabile**".
- Per i dati "***ex* sensibili**" deve essere **esplicito** e lo stesso vale rispetto a decisioni basate su trattamenti automatizzati;
- Non deve essere per forza documentato per iscritto, né è richiesta la forma scritta (anche se questa rimane la modalità più adeguata per configurare l'inequivocabilità e l'esplicitezza del consenso);
- Il Titolare del trattamento deve essere in grado di **dimostrare che l'interessato ha prestato il consenso ad un trattamento specifico (ex dati sensibili)**;
- Per i **minori** è valido a partire dai **16 anni**, prima di tale età occorre **raccogliere il consenso dei genitori** o di chi ne fa le veci.

I SOGGETTI NEL GDPR:

- **INTERESSATO**: è la persona fisica cui si riferiscono i dati personali.
- **TITOLARE DEL TRATTAMENTO**: chi determina le finalità e i mezzi del trattamento di dati personali
- **CONTITOLARE DEL TRATTAMENTO**: quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento; necessario contratto contenente le relative responsabilità in merito all'osservanza degli obblighi inerenti il trattamento e i diritti dell'interessato;
- **RESPONSABILE DEL TRATTAMENTO**: chi tratta dati personali per conto del titolare del trattamento. È responsabilità del titolare individuare un responsabile con determinate capacità e conoscenze tecniche, organizzative e con risorse adeguate per la sicurezza del trattamento (*culpa in eligendo*). I trattamenti da parte di un responsabile sono disciplinati da un contratto o da altro atto giuridico
- **D.P.O. – RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**: soggetto che dovrà vigilare affinché l'azienda dalla quale sia stato incaricato rispetti effettivamente le regole in materia di privacy allo scopo di evitare le ingenti sanzioni previste.
- **INCARICATO:** figura prevista solo indirettamente nel GDPR, quale *«persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare e del responsabile».*