Il GDPR: un percorso di fiducia

Le mosse iniziali

Molte organizzazioni si sono affrettate, a ridosso del 25 maggio scorso, a riformulare le informative secondo le previsioni dell'art. 13 del Regolamento Europeo 679/2016[i] (GDPR).

Le mosse iniziali hanno avuto due effetti, entrambi poco felici dal punto di vista degli interessati:

- le informative hanno cercato di rispettare pedissequamente le indicazioni dell'art. 13 e si sono trasformate in *lenzuoli* che pochi hanno effettivamente letto e compreso;
- l'*alluvione* di informative, arrivate tutte insieme verso la fine di maggio, ha creato un effetto repulsivo, da parte degli interessati, sia nei confronti di chi le ha inviate sia verso l'effettiva efficacia della nuova normativa in materia di dati personali.

Un aspetto positivo delle decine di informative pervenute via email è stato quello di generare la meraviglia degli interessati rispetto al numero di soggetti che erano in possesso del loro indirizzo di posta elettronica. Di fatto, tuttavia, pochi si sono preoccupati di leggere l'informativa e, semmai, di procedere a far valere i propri diritti (per esempio, invocando il diritto all'oblìo rispetto al trattamento per scopi di marketing).

Il principio di trasparenza

Lo smarrimento degli interessati poteva (e potrà) essere evitato con la lettura attenta e sistematica di tutti gli

articoli del GDPR, in particolare degli articoli iniziali. Infatti, oltre ai 173 Considerando, che spiegano quali sono gli effetti concretamente voluti dal legislatore europeo, l'articolo 5 fissa i principi che costituiscono la vera bussola dei titolari nel trattamento dei dati personali.

Tra gli altri, quelli più rilevanti, rispetto al rapporto titolare-interessato, sono il principio di trasparenza e quello di correttezza.

Il principio di trasparenza è declinabile come la possibilità da parte dell'interessato di avere il pieno controllo dei propri dati personali: sapere chi li tratta, per quale motivo, dove vanno a finire e quali strumenti giuridici esistono per rendere il trattamento conforme alle proprie esigenze e volontà.

Questo principio è talmente importante che il WP29 (oggi sostituito dall'European Data Protection Board) lo ha approfondito nelle linee guida 260 adottate in via definitiva l'11 aprile scorso[ii].

Nelle linee guida vengono sottolineati gli elementi che devono caratterizzare il comportamento trasparente del titolare in ogni interazione con l'interessato:

- le comunicazioni devono essere concise, intellegibili e facilmente accessibili;
- il linguaggio deve essere chiaro e semplice;
- il linguaggio deve essere adattato ai destinatari, in particolare se sono soggetti vulnerabili (bambini, soggetti con disabilità, stranieri, ecc.);
- le comunicazioni devono essere rese per iscritto ancorché, in casi specifici, possa essere più opportuno renderle con altri mezzi (video, audio, ecc.);
- le comunicazioni devono essere rese gratuitamente.

Queste indicazioni devono caratterizzare l'informativa di cui all'art. 13 ma anche tutte le successive comunicazioni con

l’interessato.

Il principio di correttezza

Il principio di correttezza si estende al comportamento concreto del titolare durante tutto il trattamento e va oltre la trasparenza dell’interazione titolare-interessato. È la declinazione del più generale e classico principio del *neminem laedere* (non offendere nessuno) ovvero del dovere del titolare di non arrecare danno, con comportamenti consapevoli o inconsapevoli, all’interessato.

Il rispetto di questo principio passa attraverso una chiara individuazione delle basi giuridiche poste a fondamento del trattamento ed elencate, rispettivamente, nell’art. 6 per i dati personali comuni e nell’art. 9 per le particolari categorie di dati personali (dati riguardanti la salute, le origini razziali, gli orientamenti sessuali, ecc.).

Ed il titolare deve applicare una particolare attenzione al principio di correttezza quando la base giuridica del trattamento è il consenso dell’interessato. Lo spiegano bene le linee guida 259 adottate in via definitiva il 10 aprile scorso dedicate ad approfondire le modalità di acquisizione del consenso.

Come nasce un’informativa

Rispettare il principio di trasparenza significa, innanzitutto, far nascere il rapporto titolare-interessato su basi di fiducia. Per questo, al di là dei contenuti (chiaramente stabiliti dall’art. 13), bisogna ricordare che:

- l’informativa deve essere fornita sempre;
- occorre applicare, per quanto possibile, le linee guida 260 del WP29.

Non casualmente il WP29 raccomanda, prima di tutto, un’informativa concisa cioè che non deve scoraggiarne la

lettura solo osservandone la lunghezza e non deve richiedere fatica da parte dell'interessato.

Oltre alle caratteristiche dimensionali, il titolare deve essere attento alle modalità con le quali fornisce l'informativa: occorre renderla facilmente accessibile, sia quando viene fornita dal sito web sia quando si basa su metodi più tradizionali (p.e. un apposito cartello esposto da un'officina meccanica accanto allo sportello dell'accettazione). In particolare, il WP29, per le informative sui siti web, suggerisce di strutturarle in *strati* cioè di fornire un primo livello informativo, completo ma sintetico, che può essere approfondito, tramite appositi link, secondo le esigenze dell'interessato.

Il WP29 fornisce indicazioni utili anche sul linguaggio da utilizzare. Non ispirano fiducia e, quindi, non sono segno di trasparenza le forme lessicali vaghe ed indefinite come "può", "potrebbe", "alcuni", "spesso" e le parole troppo legate alla terminologia tecnica come "backup", "firewall", "CRIF", "applicativo world check"; bisognerebbe, invece, utilizzare forme precise come "saranno comunicati", "dopo 2 anni", "ogni 3 mesi" e comprensibili dall'utente medio come "copia di riserva", "strumento di protezione della rete" e così via. Il WP29 arriva persino ad indicare un esempio di lessico da utilizzare per i minori realizzato nella stesura della "Convenzione delle Nazioni Unite sui Diritti dei Bambini nel Linguaggio dei Bambini"[iii].

Le frasi, inoltre, devono essere costruite senza troppi *giri logici* e cercando di arrivare agevolmente al concetto che si vuole esprimere.

Come chiedere il consenso

La fiducia si costruisce anche applicando buone prassi per l'acquisizione del consenso, aggiungendo ad una informazione trasparente, comunque necessaria, la correttezza dovuta nei

confronti del titolare.

Il consenso non è sempre obbligatorio perché è solo una delle possibili basi giuridiche (contratto, legge, interesse vitale, ecc.) che rendono lecito un particolare trattamento dei dati personali. Anzi, se la base giuridica è un'altra, può essere inutile e dannoso richiederlo perché può confondere le idee dell'interessato e, quindi, contrastare con un comportamento trasparente.

Tuttavia, è molto frequente che il titolare al quale forniamo i dati necessari per l'esecuzione del contratto (p.e. la piattaforma web di viaggi che ci riserva la stanza in albergo):

- non richieda il consenso per consentire l'esecuzione della sua corretta prestazione (fornendoci, però, l'informativa);
- richieda il consenso per altre finalità (p.e. per comunicazioni pubblicitarie anche tramite partner commerciale).

Questo comportamento risponde al principio di correttezza. Meno corretto, anzi illecito, è il comportamento che blocca la conclusione del contratto (la prenotazione via web) se non forniamo il consenso al trattamento per altre finalità (p.e. per comunicazioni pubblicitarie).

È per questo che il WP29 ha specificato che il consenso, qualora sia necessario al trattamento, deve essere:

- **libero**, nel senso che non ci devono essere condizionamenti dell'interessato dovuti ad una diversa forza nel rapporto (p.e. organismo pubblico-cittadino oppure datore di lavoro-dipendente);
- **specifico**, nel senso che deve essere acquisito per ogni diversa finalità; in proposito il WP29 sottolinea il concetto di *granularità* cioè di spiegazione dei singoli scopi del trattamento e di acquisizione indipendente dei

singoli consensi corrispondenti;
- **informato**, nel senso che l’interessato deve essere consapevole delle conseguenze del mancato consenso oltre che delle informazioni previste dall’art. 13;
- **non ambiguo**, nel senso che deve essere espresso con una manifestazione attiva di volontà e non, come accade in molti siti web, con l’accettazione di un segno di spunta già presente nel modulo da compilare.

Un percorso di fiducia

Conviene, quindi, essere consapevoli del percorso di fiducia tracciato dal legislatore europeo e, soprattutto, non sovrapporre sistematicamente informativa e consenso rischiando di vanificare lo spirito del GDPR.

- [i] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- [ii] http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025
- [iii] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

A cura di: **Francesco Maldera**

L’articolo Il GDPR: un percorso di fiducia proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/il-gdpr-un-percorso-di-fiducia/