Il GDPR nei contratti online

Author : Francesco Maldera

Date : 8 Maggio 2019

Il contratto: una base giuridica da esplorare

L'articolo 6 del Regolamento UE 2016/679 (GDPR) espone le basi giuridiche sulle quali fondare un trattamento lecito di dati personali da parte del titolare. Tra le sei basi giuridiche (dalla lettera a) alla lettera f) del primo paragrafo) quella che merita di essere analizzata più in profondità, nel suo concreto impiego, è quella riportata al **punto b)** e che, nella traduzione italiana, presenta il seguente testo: *"Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: […] b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; [...]"*.

È utile approfondirla perché, in molti casi, il titolare ritiene di poter trattare i dati dei propri clienti solo perché è stato siglato un contratto, ignorando **due aspetti fondamentali:**

- la base giuridica *contrattuale* (per essere brevi) non consente il trattamento indifferenziato dei dati personali riferiti ai clienti;
- con riguardo ai dati personali, nella conclusione del contratto bisogna sempre rispettare i principi di trasparenza e correttezza previsti dall'art. 5 del GDPR; in particolare, è necessario evitare di confondere il cliente (cioè l'interessato) identificando con precisione (a) quali dati personali sono *necessari all'esecuzione del contratto*, (b) quali dati personali possono essere trattati applicando altre basi giuridiche e (c) quali dati personali non devono essere trattati.

Per fare **un esempio** immediato, nel contratto tra un produttore di vini (titolare del trattamento) e il titolare di un wine bar (interessato) esistono dati personali necessari all'esecuzione del contratto (nome e cognome del titolare del wine bar, indirizzo di consegna, indirizzo email per la comunicazione delle consegne) mentre esistono dati personali, come il codice fiscale, che certamente hanno un legame con l'accordo contrattuale ma che non sono *necessari alla sua esecuzione* e la cui base giuridica del trattamento non può essere il punto b), par. 1, art. 6 del GDPR. Infatti, la base giuridica per il trattamento del codice fiscale è il cosiddetto **obbligo**

legale, esplicitato dal punto c), par. 1, art. 6 del GDPR. In realtà, persino l'indirizzo email potrebbe non essere necessario all'esecuzione del contratto perché, per esempio, una clausola prevede che le consegne avverranno sempre di martedì pomeriggio dalle 14,00 alle 16,00: non c'è bisogno dell'utilizzo della email per informare il titolare del wine bar della consegna.

Il punto b), par. 1, art. 6 del GDPR, ha una parte ulteriore che garantisce la liceità del trattamento nell'*esecuzione di misure precontrattuali adottate su richiesta dello stesso [interessato].* In realtà, è utile leggere questa parte della norma nella lingua inglese: *"in order to take steps at the request of the data subject prior to entering into a contract"*. La traduzione letterale dall'inglese (diversamente dalla versione italiana) sembra garantire la liceità quando l'interessato, di sua iniziativa, *muove passi* verso il contratto, prima di concluderlo e senza la certezza di farlo. La versione italiana, per esempio, consente al serramentista (titolare) di acquisire i dati personali riferiti alle finestre del suo potenziale cliente (interessato) per poter formulare un preventivo. Tuttavia, è solo la versione inglese che consente a una società privata (o a un Ente Locale) di utilizzare il punto b), par. 1, art. 6 del GDPR come base giuridica per la registrazione dei potenziali fornitori (interessati) alla propria piattaforma di *e?procurement*: è un passo che gli interessati fanno volontariamente verso il contratto, prima che il contratto si concluda e senza la certezza di concluderlo.

La *necessità* come fulcro dei contratti online

E se i contratti tradizionali possono essere così mutevoli da richiedere, di volta in volta, un attento esame delle basi giuridiche utili a rendere lecito il trattamento, i contratti che si concludono tramite la Rete pongono **ulteriori problematiche** legate sia alla loro specifica dinamica sia al mezzo che viene utilizzato per concluderli e, in molti casi, per eseguirli.

Il Comitato Europeo per la Protezione dei Dati Personali (European Data Protection Board)[1] ha analizzato queste problematiche nella nona riunione plenaria tenutasi a Bruxelles il 9 ed il 10 aprile scorsi, ponendo in consultazione, dal 12 aprile al 24 maggio, le *Linee guida sul trattamento dei dati personali applicando il punto b), par. 1, art. 6 del GDPR nel contesto della fornitura di servizi online agli interessati*[2].

L'elemento sul quale si fondano le linee guida è **una sorta di "test della necessità"** che aiuta il titolare a capire se i dati personali possono essere trattati basandosi sulla base giuridica contrattuale. Si tratta di comprendere bene quello che l'EDPB chiama il *fondamento logico del contratto* proponendo al titolare di interrogarsi con i seguenti **quesiti:**

1. Qual è la natura del servizio fornito all'interessato?
2. Quali sono le sue specifiche caratteristiche?
3. Qual è l'aspetto sostanziale del contratto?
4. Quali sono gli elementi essenziali del contratto?
5. Quali sono le prospettive e le aspettative delle parti del contratto?
6. Come è promosso e pubblicizzato il servizio all'interessato?
7. Un utente normale, considerando la natura del servizio, si aspetta che siano trattati i dati personali che sono richiesti dal titolare?

Il test dovrebbe fungere, quindi, da filtro per selezionare quei dati che sono giustificati dall'esecuzione del contratto. Per gli altri dati personali il titolare ha la possibilità di motivare il trattamento con altre basi giuridiche che, tipicamente, sono il **consenso** (punto a), par. 1, art. 6 del GDPR) e il **legittimo interesse** (punto f), par. 1, art. 6 del GDPR).

La specificità dei contratti online

Il test è necessario perché i contratti per la fornitura dei servizi online hanno una **caratteristica specifica:** nella maggior parte dei casi non sono frutto di una negoziazione e si concludono molto spesso con la compilazione di un *form* standard e il conseguente pagamento.

L'esempio più classico è l'acquisto di un libro da una libreria online; dopo averlo inserito nel carrello, il venditore (titolare del trattamento) chiede all'acquirente (interessato) nome, cognome, indirizzo di spedizione e indirizzo email. Nella maggior parte dei casi, se l'acquirente non compila completamente questi campi non riesce ad andare avanti nell'acquisto. In realtà, per l'esecuzione del contratto l'indirizzo email non è un dato necessario ma la scheda d'ordine è stata predisposta in modo standard e, quindi, non è adattabile alle esigenze di riservatezza che il cliente potrebbe esigere. In una libreria tradizionale questo non potrebbe mai accadere visto che il cliente potrebbe tranquillamente rifiutare di fornire dati personali al cassiere. Quindi, l'**imposizione** di indicare l'indirizzo email diventa, di fatto, un termine contrattuale che l'EDPB, prima ancora che al GDPR, ritiene **scorretto** richiamando la direttiva 93/13/EEC - *Direttiva concernente le clausole abusive nei contratti stipulati con i consumatori*[3] la quale stabilisce che *"Una clausola contrattuale, che non è stata oggetto di negoziato individuale, si considera abusiva se, malgrado il requisito della buona fede, determina, a danno del consumatore, un significativo squilibrio dei diritti e degli obblighi delle parti derivanti dal contratto"*.

L'EDPB, nelle Linee guida, non impedisce al venditore di acquisire dati personali ulteriori rispetto a quelli necessari all'esecuzione del contratto ma impone, di fatto, simulare una negoziazione, attraverso una granularità di opzioni orientate a spiegare sia la finalità dei dati acquisibili sia la rispettiva base giuridica del trattamento (diversa da quella **contrattuale** e, nella maggior parte dei casi, basata sul consenso dell'interessato).

Un'altra pratica, abbastanza frequente, analizzata nelle Linee guida, è il cosiddetto *"take it or leave it"* ovvero il tipico modello di business in cui si vendono più servizi stipulando un unico contratto e, quindi, considerando i dati personali necessari per l'esecuzione di ciascun servizio come necessari all'intero contratto. L'EDPB consiglia di verificare la necessità del trattamento per l'esecuzione di ciascun servizio e, in ossequio al principio di trasparenza, di spiegare all'interessato tali circostanze; questo anche perché se il cliente dovesse revocare uno dei servizi previsti dal contratto, il titolare, qualora non esistessero altre basi giuridiche, dovrebbe interrompere il trattamento dei dati personali che erano necessari solo a quella prestazione.

Gli effetti della tecnologia

L'EDPB, naturalmente, analizza anche gli **aspetti puramente tecnologici** della conclusione e dell'esecuzione dei contratti online, con particolare riferimento al marketing diretto (via email,

sms, ecc.) o al marketing basato sui comportamenti di navigazione. È pacifico, anche rifacendosi allo storico parere 2/2010[4] del WP29 (sulla pubblicità comportamentale) ed al documento 2/2013[5] dello stesso WP29 (sull'utilizzo del consenso per i cookie), che il titolare difficilmente potrà giustificare l'utilizzo dei dati di profilazione (e quindi anche dei rispettivi cookie) come necessari per l'esecuzione del contratto.

Esiste solo un caso, presentato nelle Linee guida, per il quale l'EDPB ritiene valido l'utilizzo dei dati di profilazione come necessari all'esecuzione del contratto: riguarda la conclusione di **contratti di personalizzazione dei contenuti**. Il capo ufficio stampa di un'azienda, per esempio, potrebbe avere interesse a ottenere, da un'agenzia di stampa, solo le notizie che riguardano il suo ambito di business e che dipendono, in parte, anche dalla sua navigazione precedente. In questo caso, è ragionevole utilizzare il punto b), par. 1, art. 6 del GDPR come base giuridica, fermo restando che la profilazione deve limitarsi alla prestazione contrattuale e non estendersi ad altre finalità (per esempio, il marketing diretto).

Conclusioni

Le Linee guida dell'EDPB sui contratti online aggiungono infine un aspetto che, spesso, più o meno consapevolmente, viene trascurato dal titolare: la **fine di un contratto**. La regola generale del GDPR prevede che il trattamento dei dati personali debba concludersi quando siano raggiunte le finalità per le quali è condotto; nel caso specifico, quindi, concluso il contratto, se non esistono altre basi giuridiche per trattare i dati del cliente, il titolare dovrebbe cancellarli. In genere, però, alcuni dati personali rimangono necessari per ragioni di fatturazione o di obblighi legali (p.e. obblighi fiscali): l'EDPB ribadisce che questi trattamenti, per il principio di trasparenza, devono essere resi noti, se possibile sin dall'inizio, all'interessato.

Possiamo, quindi, considerare queste Linee guida come il tassello mancante di un *puzzle* che era già abbastanza definito dai precedenti documenti prodotti dal WP29 sull'interazione tra utente e siti web e che i commercianti online di tutto il mondo dovrebbero conoscere.

Note:

[1] https://edpb.europa.eu/.

[2] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

[3] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:31993L0013&from=EN.

[4] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf.

[5] https://ec.europa.eu/justice/article-29/documentation/opinion-

recommendation/files/2013/wp208_en.pdf.

Articolo a cura di **Francesco Maldera** e **Giuseppe Diretto**