Il sostegno della protezione dei dati extra UE tra codici di condotta e certificazioni

Date : 3 aprile 2018

I progetti finanziati dalla Commissione Europea nell'ambito del programma Horizon2020 hanno il merito di trasformare le materie più complesse in output accessibili anche ai non addetti ai lavori, ai cittadini che non hanno dimestichezza con il settore ICT. Anche quando i tool sviluppati non sono progettati per un impiego d'uso quotidiano, però, il loro merito è quello di sostenere i diritti fondamentali a partire dall'operatività delle aziende.

In particolare, il progetto Privacy Flag [1], che si avvia alla conclusione della sua ricerca iniziata nell'aprile 2015, intende sviluppare una struttura di protezione della privacy collettiva che consenta ai cittadini di controllare e proteggere meglio i propri dati personali. Oltre a una serie di strumenti e soluzioni che consentono agli interessati di valutare collettivamente e controllare il livello di rischio per la loro privacy nel contesto di applicazioni web, app per smartphone e Internet of Things, Privacy Flag fornisce anche un meccanismo volontario di *compliance*, ma legalmente vincolante, messo a disposizione per le aziende situate al di fuori dell'Europa.

L'obiettivo è quello di consentire a imprese cinesi, giapponesi, sud coreane e americane di allinearsi e rispettare gli standard europei in termini di protezione dei dati personali. Il Voluntary Compliance Commitment tool (di seguito, "VCT") si basa su un accordo unilaterale che, attraverso la sottoscrizione volontaria della società mediante firma elettronica, rende questo impegno all'osservanza del GDPR efficace, fornendo una base giuridica che consenta a terzi di farvi riferimento in caso di non conformità.

Nel corso dei mesi, considerato che il tool è nato nella vigenza della Direttiva 95/46/CE ed è stato poi riadattato all'adozione del GDPR, si è osservato come tale meccanismo possa costituire una valida alternativa per sostenere e dimostrare un livello adeguato di protezione dei dati fornito dai titolari del trattamento al fine di rispettare il celebre principio dell'*accountability* introdotto proprio dal GDPR, apportando peraltro, ulteriori benefici che aumenteranno la fiducia degli utenti nelle attività delle imprese extra UE.

Ma andiamo con ordine.

Innanzitutto, l'adozione formale di questo "strumento di impegno volontario alla conformità"

consente di sottoporre le imprese situate a distanza geografica e culturale a un insieme comune di norme allineate alla regolamentazione europea sulla protezione dei dati personali.

L'accordo unilaterale si basa su una *fee* proporzionata alle dimensioni dell'azienda ed è strutturato sulla base di clausole contrattuali standard per trasferimenti da titolari/responsabili a titolari/responsabili stabiliti al di fuori dell'UE (cfr. Model clauses della Commissione Europea [2]). Inoltre, considerando la possibilità per le società straniere di stabilire una controllata all'interno dell'UE, il VCT è stato definito seguendo il modello BCR (Binding Corporate Rules), inteso come soluzione per le società multinazionali che esportano dati personali dallo Spazio economico europeo ad altre entità del gruppo situate in paesi terzi che non garantiscono un livello adeguato di protezione.

Lo scopo del VCT è quello di vincolare il titolare del trattamento dei dati (la Società che sottoscrive il contratto) a una serie di obblighi che si applicano a favore degli interessati. Infatti, le clausole dell'accordo unilaterale riprendono tutti i principi di base della legislazione europea sulla protezione dei dati personali quali il principio di liceità del trattamento, di minimizzazione, di limitazione delle finalità, dell'esattezza, dell'integrità, della riservatezza nonché l'obbligo del titolare di fornire le informazioni, la notifica della violazione dei dati, ecc.

Ciò che rende il tool effettivamente molto semplice da utilizzare, il fatto di essere stato reso disponibile come piattaforma contrattuale online all'indirizzo www.privacypact.com. La stessa piattaforma mette a disposizione un elenco pubblico contenente i dettagli delle organizzazioni che hanno deciso di sottoscrivere l'accordo, al fine di renderli conoscibile agli interessati.

Una volta effettuata la registrazione dell'azienda da parte di un soggetto interno autorizzato, si firmerà digitalmente il contratto che avrà una validità di dodici mesi. Al termine di tale periodo, l'accordo potrà essere rinnovato dietro pagamento di una piccola tassa di rinnovo, ammettendo comunque la revoca del contratto in qualsiasi momento da parte dell'azienda – in tal caso, conseguentemente rimossa dalla lista pubblica.

A beneficio dei sottoscrittori, inoltre, firmando il contratto, Privacy Flag rilascia un sigillo apponibile sui siti web dell'azienda, che dimostra l'impegno volontario della società a rispettare i principi cardine della protezione dei dati.

Non volendosi sostituire in alcun modo alle autorità nazionali per la protezione dei dati, Privacy Flag non è responsabile per la risoluzione delle controversie tra *data subject* e aziende firmatarie. Tuttavia, il sito permette agli utenti di effettuare segnalazioni documentando la decisione di un'Autorità per la protezione dei dati che identifica una delle società pubblicate nella lista come non conforme alle norme sulla privacy dell'UE. Qualora tale decisione sia stata presa, vi è la cessazione automatica dell'accordo con la società, cui consegue anche la rimozione del sigillo di partecipazione.

Ma perché sottoscrivere il VCT se il GDPR "*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” (Art. 3(2)?

Ebbene, il VCT rappresenta un prezioso strumento aggiuntivo volto a garantire il rispetto delle norme sulla protezione dei dati personali da parte di tutte le entità situate al di fuori dell'UE in tre diversi casi:

- se non offrono beni e servizi ai cittadini dell'UE o non controllano ancora il loro comportamento, ma attraverso la sottoscrizione volontaria si impegnano a rispettare le norme europee sulla protezione dei dati personali in previsione dell'offerta di beni e servizi o del monitoraggio del comportamento;
- se trattano dati personali di persone fisiche che non sono nell'UE (ma potrebbero essere cittadini dell'UE) offrendo beni e servizi o svolgendo attività di monitoraggio sul comportamento, anche se il comportamento non si svolge all'interno dell'Unione;
- se desiderano offrire beni e servizi ai cittadini dell'UE o monitorarne il comportamento e sono alla ricerca di uno strumento di responsabilizzazione per offrire anche visivamente (con il sigillo) garanzie in relazione alla tutela della vita privata, dei diritti e delle libertà fondamentali e l'esercizio dei diritti correlati.

Per inquadrare il contesto normativo in cui il VCT opera è bene ricordare che il GDPR consente esplicitamente la possibilità per "*responsabili del trattamento o incaricati del trattamento che non sono soggetti al presente regolamento a norma dell'articolo 3 al fine di fornire garanzie adeguate nell'ambito dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*" a "*rendere impegni esecutivi, tramite strumenti contrattuali o altri strumenti giuridicamente vincolanti, per l'applicazione di tali garanzie adeguate anche in relazione ai diritti degli interessati* " (articolo 40.3).

Inoltre, al fine di migliorare la trasparenza e l'osservanza del GDPR, il legislatore europeo ha incoraggiato l'istituzione di meccanismi di certificazione della protezione dei dati e di sigilli e marchi di protezione dei dati, in particolare per consentire ai dati di valutare rapidamente il livello di protezione dei dati dei prodotti pertinenti e servizi.

Questo è il motivo per cui, conformemente all'articolo 42 del GDPR ed esattamente come per i codici di condotta, "*i responsabili del trattamento o i trasformatori che non sono soggetti al presente regolamento a norma dell'articolo 3 nell'ambito dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*" possono "*assumere impegni vincolanti e esecutivi, tramite strumenti contrattuali o altri strumenti giuridicamente vincolanti, per applicare tali garanzie appropriate, anche in relazione ai diritti degli interessati*".

Grazie a questo nuovo background legale, dunque, il progetto Privacy Flag ha dato vita a un vero e proprio meccanismo aggiuntivo di protezione dei dati, in conformità con gli articoli 40(3) e 42(2) del GDPR. Così, pur non costituendo il VCT una certificazione (articolo 42) o un codice di condotta (articolo 40), esso rappresenta a tutti gli effetti uno strumento valido per il supporto e la dimostrazione del principio di *accountability ex* art. 5(2), GDPR.

Il VCT può essere visto, allora, come un ibrido tra un codice di condotta – dal momento che contiene una serie di principi e obblighi per il responsabile del trattamento dei dati che ne fa parte – e una certificazione, poiché garantisce anche l'identificazione positiva delle aziende aderenti con un elenco pubblico e attraverso un sigillo che la Società può ottenere dopo la conclusione del contratto. Ecco che H2020 ha dato origine a una “certificazione di condotta”.

Bibliografia

- [1] www.privacyflag.eu
- [2] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
- [3] Regolamento (UE) 2016/679 in http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679

A cura di: **Camilla Bistolfi**