LS NEWSLETTER

IT Law & Data Protection

Agosto 2022

Il Garante per la protezione dei dati personali italiano ha detto stop all'uso di Google Analytics

Con comunicato stampa dello scorso 23 giugno, il Garante per la Protezione dei dati personali italiano ("**Garante**") ha dichiarato che ogni sito web che utilizza il servizio Google Analytics ("**GA**"), senza le garanzie previste dal Regolamento (UE) 2016/679 ("**GDPR**") viola la normativa sulla protezione dei dati personali in quanto trasferisce i dati degli utenti negli Stati Uniti, Paese privo di un adeguato livello di protezione.

La problematica relativa al trasferimento dei dati personali verso paesi extra – UE non è certamente nuova.

Già a luglio 2020, la Corte di Giustizia dell'Unione europea ("**CGUE**") ha sancito il divieto di trasferimento dei dati personali di cittadini europei negli Stati Uniti – in assenza di misure giuridiche, tecnologiche e organizzative, in grado di eliminare i rischi per la *privacy* – e ha dichiarato invalido l'accordo UE-USA definito "**Privacy Shield**".

La decisione del Garante è l'esito di una istruttoria avviata in coordinamento con altre autorità privacy europee a seguito della presentazione, da parte dell'associazione NOYB – European Center for Digital Rights, di 101 reclami relativi ad aziende europee, di cui quattro italiane, ritenute in violazione del GDPR.

- Provvedimento del Garante austriaco del 22 dicembre 2021

L'Autorità Garante austriaca ("**DSB**") ha sanzionato il titolare di un sito web che impiegava Google Analytics al fine di generare valutazioni statistiche sul comportamento dei visitatori.

Secondo la DSB, Google Analytics non rispetta le regole dettate dal Regolamento (UE) 2016/679 ("**GDPR**") sul trasferimento dei dati, in quanto le misure tecniche, organizzative e contrattuali adottate da Google non sono sufficiente a tutelare i diritti degli utenti.

Il DSB ha, in primo luogo, analizzato i dati personali oggetto di trattamento al fine di verificare se questi costituissero dati personali ai sensi dell'art. 4, par. 1, GDPR.

Secondo il DSB, si tratta di dati personali in quanto:

- pur essendo dati anonimizzati, Google – attraverso i *cookie* che vengono depositati sul dispositivo – è in grado di abbinare l'account Google dell'utente che visita il sito al dato anonimizzato;
- gli identificativi online univoci possono essere abbinati con altri dati, permettendo così la ricostruzione dell'impronta del *browser* che consente una sufficiente identificazione dell'utente;

Pertanto, Google Analytics tratta dati personali e li trasferisce al di fuori del territorio europeo.

Nel caso di specie, il trasferimento è basato sulle clausole contrattuali standard, alle quali Google ha aggiunto ulteriori misure al fine di raggiungere un livello adeguato di sicurezza, quali la cifratura dei dati. Secondo il Garante austriaco tale misura non è sufficiente a garantire la tutela dei dati personali in quanto Google – responsabile del trattamento – per operare il trattamento per conto del titolare deve accedere ai dati, ed è quindi in possesso delle chiavi di decifrazione.

- Provvedimento del Garante francese del 10 febbraio 2022

Sulla stessa linea, l'Autorità Garante francese (CNIL), con pronuncia del 10 febbraio 2022, ha rilevato come Google Analytics raccolga informazioni relative all'utente, dati personali ai sensi

dell'art. 4, par. 1, GDPR, ma non sia in grado di garantire che tali informazioni rimangano sul territorio UE.

Il rischio – rilevato dal CNIL come anche dal DSB – è che le informazioni esportate negli Stati Uniti possano essere oggetto di acquisizione anche da parte delle autorità statunitensi, e in particolare dei loro servizi di *intelligence*.

- **Provvedimento del 9 giugno 2022 del Garante italiano [doc. web n. 9782890]**

Lo scorso 9 giugno, il Garante per la protezione dei dati personali italiano ("**Garante**") ha ammonito la società Caffeina Media S.r.l., gestore del sito web, in quanto ha considerato illecito il trattamento dei dati personali degli utenti del sito web posto in essere per il tramite di Google Analytics, ingiungendo di conformarsi al GDPR entro di 90 giorni.

Nel provvedimento ha ribadito come:

- I dati raccolti, quali indirizzo IP del dispositivo dell'utente e informazioni relative al browser, sistema operativo, lingua selezionata, nonché data e ora della visita al sito web, vengano trasferiti attraverso Google Analytics a Google LLC, con sede negli Stati Uniti;
- Le informazioni esportate negli Stati Uniti possano essere oggetto di acquisizione anche da parte delle autorità statunitensi;
- L'indirizzo IP costituisce un dato personale che anche nel caso fosse parzialmente oscurato non costituirebbe un dato anonimo, data la capacità di Google di arricchirlo con altri dati di cui è in possesso.

Tutti i titolari del trattamento dovrebbero verificare la conformità delle modalità di utilizzo degli strumenti di tracciamento utilizzati sui propri siti web con la normativa in materia di protezione dei dati personali.

Certamente ci si aspetta che il Garante proceda, sulla base di specifiche attività ispettive, a verificare la conformità al GDPR dei trasferimenti di dati effettuati dai titolari.

COSA FARE A SEGUITO DEL PROVVEDIMENTO DEL GARANTE:

In prima battuta è sempre importante ricordarsi del concetto di **accountability** introdotto dal GDPR. Questo principio risulta ancora oggi di difficile comprensione e applicazione pratica in quanto è necessario (per tutti gli operatori del settore) passare da un sistema impositivo/dispositivo ad un sistema di principi generali e linee guida (più o meno specifiche) a cui accedere con valutazioni e misura personalizzate sulla base della realtà aziendale che ci si trova a gestire.

- In primis consigliamo a tutti **l'immediato passaggio a Google Analytics 4 (GA4)** che pur non risolvendo i problemi di fondo sollevati dal Garante costituisce un indubbio passo avanti in termini di compliance al GDPR. Il mero passaggio a GA4 non sarà però sufficiente, si tratterà di impostare l'utilizzo del tool di Mountain View in modo da poterne motivare la scelta anche (e soprattutto) in termini di misure tecniche ed organizzative adottate. (N.B. anche GA4 pur presentando maggiori tutele e misure volte alla sicurezza dei dati personali, non sembra evitare il "problema" principale del trasferimento dei dati all'estero e della loro riconducibilità al singolo soggetto interessato).

- Per quelle organizzazioni che dovessero decidere di continuare ad adottare il tool *Google* (GA4) riteniamo indispensabile, quantomeno, implementare le misure tecniche ed organizzative:

- richiesta del consenso in base all'art. 49 lett. a) del GDPR, ricordando che affinchè il consenso possa dirsi validamente prestato è necessario rispettare i principi sintetizzati nella seguente info grafica:

- **Anonimizzazione dei dati trasferiti** (in particolare l'indirizzo IP dell'interessato). Questa soluzione implementabile con GA4 (le versioni precedenti lo consentivano ma sono state dichiarate espressamente no compliance) può certamente costituire una di quelle misure di accountability sopra richiamate, ma persistono dubbi sul fatto che Google possa comunque essere in grado di risalire all'identità del soggetto interessato.

- Per i molti che troveranno oggettive difficoltà o non saranno in grado di giustificare la scelta di mantenere il tool di Google consigliamo di iniziare a valutare **l'implementazione di tool alternativi**, tra questi in particolare il CNIL francese consiglia *Matomo* disponibile sia in versione *cloud* che in versione *on premise* (ossia con installazione del tool sui propri server). Con la soluzione on premise, dunque, si manterrebbe il controllo effettivo sui dati raccolti, evitando ogni trasferimento all'estero e gestendo la loro sicurezza in prima linea. Chi non si è dotato di un reparto IT o di consulenti esterni che possano gestire la soluzione *on premise di Matomo*, può acquistare una licenza di *Matomo cloud*, di modo da sfruttare i server europei della società e monitorare, così, il traffico e le campagne di Google Ads senza troppi sacrifici.

Decreto trasparenza (Decreto Legislativo n.104 del 27 giugno 2022) in recepimento della Direttiva (UE) 2019/1152

In recepimento della Direttiva (UE) 2019/1152 relativa alle condizioni di lavoro trasparenti e prevedibili nell'Unione europea, il 29 luglio 2022 è stato pubblicato in Gazzetta Ufficiale il Decreto

Legislativo n.104 del 27 giugno 2022, il quale ha come obiettivo quello di garantire la conoscenza delle condizioni di lavoro a tutti i lavoratori.

Il Decreto trasparenza – che si applica a tutti i contratti di lavoro subordinato, al mondo delle Agenzie per il Lavoro e alle collaborazioni coordinate e continuative – introduce degli obblighi specifici in capo al datore di lavoro:

- Art. 1 *bis* comma 1: obblighi di informazione circa l'utilizzo di sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini dell'assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori.

Tali informazioni devono essere rese in modo trasparente, in formato strutturato, di uso comune e leggibile da dispositivo automatico. Inoltre, il lavoratore ha diritto a richiedere ulteriori informazioni sull'impatto di tali sistemi automatizzati sul rapporto di lavoro e il datore di lavoro è tenuto a dare risposta entro 30 giorni.

- Art. 1 *bis* comma 2: obblighi di integrazione dell'informativa privacy con le istruzioni per il lavoratore in merito alla sicurezza dei dati e l'aggiornamento del registro dei trattamenti.

Al fine di verificare la conformità al GDPR degli strumenti utilizzati, il datore di lavoro deve effettuare un'analisi dei rischi e una valutazione d'impatto degli stessi trattamenti.

In assenza, ritardo o incompletezza delle comunicazioni previste dal Decreto trasparenza sono previste sanzioni differenziate per la tipologia di omissione. La sanzione ordinaria prevede per il datore di lavoro una sanzione amministrativa pecuniaria da 250 a 1.500 euro per ogni lavoratore interessato.

Lorenzo Bianchi

Partner

l.bianchi@lslex.com