GDPR: Un'evoluzione, non una rivoluzione

Liberatoria legale
Questo articolo non costituisce parere legale, né queste informazioni intendono creare o far nascere un qualsiasi rapporto avvocato-cliente.
Se necessario, per un parere professionale è opportuno rivolgersi a un legale competente.

Introduzione

Il Regolamento generale sulla protezione dei dati (General Data Protection Regulations, GDPR) sostituisce la Direttiva esistente sulla protezione dei dati del 1995, armonizzando le varie leggi sulla privacy dei dati esistente in tutti i 28 stati membri dell'UE.

Fin dagli inizia della nostra attività in Europa nel 2005, la tecnologia di Criteo ha sempre operato ai massimi livelli di privacy e sicurezza dei dati, continuando a dare la possibilità ai nostri clienti di rispondere alle aspettative dei consumatori con pubblicità personalizzate e rilevanti. Come azienda globale con uffici in diversi Paesi europei e che lavora con migliaia di clienti della pubblicità e partner editori, i cui clienti e utenti risiedono nell'Unione Europea, siamo abituati a rispettare i requisiti di ogni Paese, in tutto il mondo.

È convinzione di Criteo che la coerenza e la certezza riguardo alla privacy e alla tutela dei dati non possano che portare benefici alle aziende e ai consumatori. Questo è il motivo per cui Criteo si impegna per la conformità al GDPR e per cui stiamo lavorando con clienti e partner soggetti alle nuove normative, offrendo loro supporto e condividendo best practice per gestire al meglio la transizione. Noi di Criteo siamo pronti ad accogliere la sfida del GDPR e prevediamo un impatto ridotto della nuova normativa sulla capacità dei nostri clienti e partner di lavorare con noi.

Nel complesso, quest'aggiornamento normativo è un'evoluzione che allinea le politiche di tutela dei dati di tutti gli stati membri dell'UE offrendo coerenza di applicazione e di esecuzione da parte delle autorità preposte alla tutela dei dati (Data Protection Authorities, DPA) in ogni stato membro dell'UE. Gli obiettivi del GDPR sono chiari:

- Modernizzare il sistema giuridico per proteggere i dati personali in un'era di globalizzazione e di innovazione tecnologica.

- Rafforzare i diritti dell'individuo riducendo i carichi amministrativi per garantire un flusso libero di dati personali all'interno dell'UE.
- Fare chiarezza e dare coerenza per quanto riguarda le regole di tutela dei dati personali e garantire un'applicazione coerente e un'efficace implementazione in tutta la UE.

Che cosa sono questi "dati personali" così come definiti dal GDPR?

Il GDPR protegge la privacy dei cittadini UE ed è valido per tutte le aziende che raccolgono o elaborano dati personali riguardo a individui dell'Unione Europea, anche se l'azienda non ha sede nell'Unione Europea. Una significativa conferma per il settore del marketing digitale è che il GDPR è valido per qualsiasi informazione relativa a una persona fisica identificata o identificabile, e ciò comprende identificatori online, quali gli ID dei cookie e della pubblicità mobile. Questi identificatori online vengono ora citati esplicitamente nella definizione di "dati personali", a conferma dell'interpretazione in senso più ampio di dati personali già in presente nelle leggi dell'UE.

È importante notare che questi identificatori online erano già considerati dati personali da molte DPA europee. Per Criteo questo requisito non rappresenta una novità dal momento che noi raccogliamo dati personali non sensibili sotto forma di cookie. Noi, perciò, conosciamo bene queste distinzioni, e seguiamo metodi collaudati per la conformità, pur continuando a garantire performance ai nostri clienti.

Vi sono delle domande che tutte le aziende si fanno e che riguardano la gestione dei dati. Per prima cosa, che cosa sono questi "dati personali", così come definiti dal GDPR? I dati personali sono qualsiasi cosa che contenga:

- *Informazioni che identifichino direttamente*, quali il nome di una persona, il suo numero di telefono, ecc.
- *Dati pseudonimi o informazioni non direttamente identificanti*, che non consentono di identificare gli utenti in modo diretto ma permettono di riconoscere comportamenti individuali (ad esempio per mostrare l'annuncio giusto all'utente giusto al momento giusto).

Il GDPR stabilisce una chiara distinzione tra informazioni direttamente identificanti e dati pseudonimi. Esso incoraggia l'uso di informazioni pseudonime e prevede espressamente: "l'applicazione di pseudonimizzazione ai dati personali può ridurre i rischi per i soggetti interessati e può aiutare i titolari e i responsabili del trattamento a rispettare gli obblighi di tutela dei dati".[1]

I dati che Criteo raccoglie ed elabora per i suoi clienti e partner non possono essere qualificati come sensibili secondo la definizione del GDPR. Qual è la definizione di "dati sensibili"? Tutti quei dati che rivelano:

- Origine razziale o etnica

[1] *General Data Protection Regulation – Whereas (28)*

- Opinioni politiche
- Credi religiosi o filosofici
- Associazione a sindacati
- Dati genetici
- Dati biometrici con lo scopo di identificare in modo esclusivo una persona fisica
- Dati che riguardano la salute o la vita sessuale e/o l'orientamento sessuale di una persona fisica

Criteo raccoglie e tratta per i suoi clienti e partner identificatori pseudonimi online legati a eventi di navigazione. Lavorando con Criteo, i nostri clienti e partner necessitano solo di accedere a dati pseudonimi che non consentono la diretta identificazione di utenti. Questi dati pseudonimi includono:

- ID di cookie
- Indirizzi e-mail criptati
- ID di pubblicità mobile
- Qualsiasi altro identificatore tecnico che consenta a Criteo di individuare il comportamento personale senza identificare direttamente l'individuo.

Qual è la differenza tra consenso non ambiguo e consenso esplicito?

Il GDPR stabilisce anche una chiara distinzione tra il consenso valido e non ambiguo e il consenso esplicito della persona. Mentre entrambe le forme di consenso richiedono un atto positivo da parte della persona, il consenso esplicito implica una stretta interpretazione di ciò che costituisce questa azione positiva da parte dell'utente (ad es., spuntare una casella, fare clic su un pulsante con la dicitura "Accetto"). Ciò si applica unicamente ai dati personali sensibili, quali razza, religione, orientamento sessuale, affiliazione politica e stato di salute. È importante notare che gli solo identificatori online (ad es. i cookie) vengono considerati dati personali non sensibili, per cui non è necessario esprimere un consenso esplicito.

Questo che cosa significa e come si applica alla tua attività? Il GDPR fornisce sei basi legali della raccolta e del trattamento dei dati in Europa. Quindi, se si raccolgono dati personali di qualsiasi genere, la raccolta deve avere basi legali. Le sei basi legali sono le seguenti:

- L'interesse vitale dell'individuo
- L'interesse pubblico
- L'esigenza contrattuale
- La conformità a obblighi legali

- Il consenso valido e non ambiguo dell'individuo
- L'interesse legittimo del titolare del trattamento

È importante notare che tutte queste basi giuridiche hanno lo stesso valore legale, il che significa che sono autonome ed esclusive, l'una rispetto all'altra. Per le attività dei settori del marketing o del marketing digitale o per coloro che raccolgono dati a scopo di marketing, le due basi legali che potrebbero applicarsi sono: (1) il consenso valido e non ambiguo dell'individuo e 2) l'interesse legittimo del titolare del trattamento.

La nostra opinione è che la base che si applica maggiormente ai nostri clienti e partner che raccolgono dati personali, identificatori online compresi, è quella del consenso valido e non ambiguo.

Il consenso alla raccolta per il retargeting mediante cookie rappresenta la regola in Europa sin dal 2009, e con l'adozione della Direttiva sulla ePrivacy (cioè la direttiva sui cookie). I clienti e gli editori partner di Criteo, che non elaborano dati sensibili ma lavorano piuttosto con dati relativi alla navigazione web, alle intenzioni di acquisto e alla cronologia degli acquisti collegati a identificatori tecnici pseudonimi, hanno già maturato l'abitudine di conformarsi a tali requisiti.

Prevediamo che le regole sul consenso valido e non ambiguo rappresenteranno un'evoluzione delle leggi già molto protettive esistenti in Europa. La CNIL (Commission nationale de l'informatique et des libertés, autorità francese per la protezione dei dati e autorità di supervisione di Criteo) fornisce le stesse raccomandazioni per la raccolta del consenso degli utenti[2] e raccomanda diverse soluzioni tecniche di facile utilizzo che gli amministratori di siti Web possono implementare.

Le condizioni richieste dal GDPR per un consenso valido e non ambiguo sono molto simili, se non identiche, alle condizioni già specificate in passato dal Gruppo di lavoro dell'Articolo 29[3]:

> ***Informazioni specifiche:*** *"Per essere valido, il consenso deve essere specifico e basarsi su informazioni appropriate fornite all'individuo. In altre parole, il consenso generale senza specificare lo scopo esatto del trattamento dei dati non è accettabile."*
>
> ***Tempistiche:*** *"Come regola generale, il consenso deve essere dato prima dell'inizio del trattamento dei dati."*
>
> ***Scelta attiva:*** *"Il consenso deve essere non ambiguo. Perciò, la procedura di chiedere e dare il consenso non deve lasciare nessun dubbio riguardo alle intenzioni del soggetto. In linea di principio, non esistono limiti alla forma che il consenso può assumere. Tuttavia, perché il consenso sia valido, i desideri dell'utente devono essere indicati in modo attivo. L'espressione minima di un'indicazione potrebbe essere*

---

[2] *CNIL: "Cookie - come rendere conforme il mio sito Web" https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite*
[3] *Article 29 Working Party – 2013 Guidance on obtaining consent for cookies: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf*

qualsiasi tipo di segnale abbastanza chiaro da essere in grado di indicare i desideri del soggetto titolare dei dati e da essere compreso dal titolare del trattamento."

Dato liberamente: *"Il consenso può essere valido solo se il soggetto titolare dei dati è in grado di esercitare una vera scelta e non vi è il rischio di inganno, coercizione o significative conseguenze negative."*

Come si applica "l'interesse legittimo del titolare del trattamento"?

Perché l'interesse sia legittimo, lo scopo del trattamento dei dati deve essere ragionevolmente previsto dagli utenti. L'elaborazione di dati personali per scopi di marketing diretto può essere vista come un interesse legittimo e come tale eseguita. Tuttavia, questo interesse legittimo non può prevalere sui diritti fondamentali della privacy degli utenti ed è necessario implementare misure di sicurezza appropriate per limitare i potenziali rischi per la privacy degli utenti.

Le norme basilari da soddisfare prima di cercare di rivendicare un interesse legittimo sono:

- Una spiegazione di quali dati vengono raccolti, lo scopo specifico di tale raccolta, oltre che il modo con cui influisce sull'esperienza di navigazione online. Ad esempio:

  "Il nostro [sito Web] / la nostra [app] utilizza cookie/ID pubblicitari a fini pubblicitari. Questo ci consente di mostrare i nostri annunci ai visitatori che sono interessati ai nostri prodotti anche su siti Web e app di partner. Le tecnologie di retargeting utilizzano i vostri cookie o ID pubblicitari e mostrano gli annunci in base al vostro comportamento di navigazione. Per approfondire e/o opporsi tali servizi, vi preghiamo di fare riferimento all'informativa sulla privacy elencata qui di seguito." [Aggiungere il link alla Politica sulla privacy del vostro partner. Ad esempio, la Politica sulla privacy di Criteo è all'indirizzo: http://www.criteo.com/it/privacy/ *]*

- Un modo per gli utenti di controllare la propria esperienza, che includa un'opzione di rinuncia di facile accesso e utilizzo, e una chiara spiegazione di come ciò influirà sull'esperienza pubblicitaria di chi naviga.
- Facile accesso a un'informativa sulla privacy, oltre che a informazioni su qualsiasi standard o impegno del settore sulla privacy adottato dalla vostra azienda. Ad esempio: Criteo è membro della Network Advertising Initiative.

Ci sono alcune domande chiave a cui ogni azienda deve essere in grado di rispondere per stabilire se esiste un interesse legittimo:

- Qual è lo scopo dell'operazione?
- È necessario soddisfare uno o più obiettivi organizzativi specifici?
- Il GDPR o altre normative identificano specificamente l'attività di trattamento come legittima, soggetta al completamento di un test di bilanciamento e a un risultato positivo?

- Esiste un altro modo di ottenere l'obiettivo?
- L'individuo si aspetta che si verifichi l'attività di elaborazione?
- Qual è la natura dei dati da elaborare? Questo tipo di dati ha speciali tutele da parte del GDPR?
- Il trattamento dei dati limiterebbe o pregiudicherebbe i diritti dei singoli?
- La persona riceve un avviso corretto sul trattamento? Se sì, come? È sufficientemente chiaro e preciso riguardo le finalità dell'elaborazione?

Qual è l'approccio di Criteo alla privacy dei dati?

Alla Criteo la privacy è un principio guida. Facciamo di tutto per proteggere e per trattare i dati conformemente alle leggi in vigore sulla privacy e sulla protezione dei dati. E questo comprende il GDPR.

I nostri team prodotto sviluppano ciascuna funzione non dimenticando mai la privacy: è il fondamento di Privacy by Design, il nostro sofisticato approccio che garantisce un livello di sicurezza leader del settore, tanto per i commercianti quanto per i consumatori.

Privacy by Design rappresenta la pratica e l'impegno di lunga data di Criteo per garantire a consumatori e marketer livelli di privacy e sicurezza leader del settore. Tra gli elementi chiave:

- Come richiesto dal GDPR, dal 2013 abbiamo un funzionario addetto alla privacy dei dati, affiancato da un team di esperti della privacy.
- Questi esperti fanno parte dell'organizzazione che si occupa di Prodotto e R&S. Eseguono costantemente valutazioni dell'impatto sulla privacy per monitorare potenziali rischi durante il ciclo di vita del prodotto e mitigarli in modo proattivo.
- Il team della privacy dei dati offre formazione a tutta l'azienda, fa applicare i codici di condotta e si impegna a garantire che i nostri prodotti e servizi siano i migliori.
- Rivediamo e documentiamo regolarmente le nostre politiche interne, se necessario correggiamo le politiche sulla privacy esistenti, e le applichiamo con i nostri partner e venditori.

Severe misure di sicurezza

Come richiesto dal GDPR, noi di Criteo adottiamo già severe misure di sicurezza quando raccogliamo i dati dei consumatori dai nostri clienti. Utilizziamo metodi pseudonimi moderni, compresi i processi di doppio hashing MD5 e SHA-256, che possono essere considerati best practice previste dal GDPR, e non memorizziamo mai volontariamente informazioni personali che identifichino i singoli consumatori. Per motivi di compliance e di ottimizzazione della performance, memorizziamo dati dei consumatori UE nel centro dati europeo fisicamente più vicino a loro.

Opzioni sugli annunci: attenzione ai diritti e al controllo da parte dei consumatori

Criteo ha da tempo riconosciuto la necessità di trovare un equilibrio tra esperienze pubblicitarie pertinenti e le aspettative sulla privacy, pur consentendo ai consumatori di avere il controllo sulle proprie esperienze. I consumatori comprendono questo compromesso. Per questo motivo Criteo si è impegnata nel programma di "opzioni sugli annunci" fin dal 2008, per consentire ai consumatori di vedere con un solo clic esattamente dove Criteo usa i dati e come protegge la loro privacy. Quando un consumatore sceglie esplicitamente di negare il suo consenso, noi interrompiamo immediatamente il tracciamento e il retargeting. Quindi, rimuoviamo tutti gli identificatori dai suoi browser, rendendo impossibile il retargeting per il futuro. In accordo con le normative UE sulla tutela dei dati, i dati raccolti sui consumatori vengono conservati solo per 13 mesi.

La leadership del settore: investire in standard e certificazioni

Abbiamo già implementato un grande numero di certificazioni che vengono riviste ogni anno da enti normativi e di revisione, tra cui:

- Network Advertising Initiative Standards
- IAB Europe
- Principi di autoregolamentazione per la pubblicità comportamentale online della Digital Advertising Alliance (DAA)
- Principi di autoregolamentazione della European Digital Advertising Alliance (EDAA)
- Principi di autoregolamentazione della Digital Advertising Alliance of Canada
- Certificazione TrustArc Trusted Data Collection

Quali sono le tue responsabilità?

Il GDPR esige dalle aziende che raccolgono dati all'interno dei Paesi dell'UE di conformarsi alle nuove normative, che interessano la protezione e la sicurezza dei dati. Questo si applica anche alle imprese globali con sede al di fuori dell'UE, se si rivolgono a un'audience dell'UE. Il GDPR costituisce un vantaggio per la propria azienda perché consolida le varie leggi di protezioni sulla privacy dei dati che esistono in tutti i 28 stati membri. Ecco perché Criteo sta aiutando i nostri clienti e partner a verificare se conoscono quali procedure seguire per conformarsi essi stessi al GDPR. Ecco alcune best practice da prendere in considerazione per iniziare il percorso verso la conformità:

Nominare un responsabile per la protezione dei dati (RPD)

Il GDPR richiede la nomina di un Responsabile della protezione dei dati (Data Protection Officer, DPO) in ogni caso in cui:

- il trattamento venga eseguito da un'autorità pubblica o un ente pubblico, a eccezione dei tribunali che agiscono nell'esercizio delle proprie funzioni giudiziarie;
- le principali attività di titolare o di responsabile del trattamento consistano in operazioni di trattamento che, per loro natura, loro ambito e/o loro scopo, richiedano un monitoraggio regolare e sistematico dei soggetti dei dati su larga scala; oppure
- le principali attività di titolare o di responsabile del trattamento consistano nel trattamento su larga scala di dati sensibili (dati che rivelano l'origine razziale o etnica, le opinioni politiche, le opinioni religiose o filosofiche, le condizioni di salute o l'orientamento sessuale, ecc.) o i dati personali relativi a condanne politiche o a reati.

Questo ruolo monitorerebbe e gestirebbe sia i dati sia le operazioni necessarie mediante le normative. Inoltre, il RPD dovrebbe provare che essi non presentano conflitti di interesse per quanto riguarda la protezione dei dati per la propria organizzazione.

Accertarsi che il proprio RPD sia pronto a collaborare

I dipendenti sono l'elemento migliore per poter comprendere quali potrebbero essere le attuali mancanze delle politiche sulla protezione dei dati della propria azienda. Accertarsi che il RPD, i team legale, il team IT e quello per la conformità abbiano una conoscenza chiara e completa delle pratiche di tutela dei dati dell'azienda. Essi devono lavorare insieme per contribuire a creare un processo per la conformità per cui la loro organizzazione raccolga i dati in modo collaborativo.

Fornire trasparenza e controllo

Il linguaggio delle informazioni e del consenso che si forniscono ai propri clienti deve essere il più chiaro e trasparente possibile. Il proprio sito Web deve rendere esplicitamente chiaro con esattezza quello per cui i clienti hanno dato o non hanno dato esplicitamente il loro consenso, ed esattamente quali tipi di dati essi stanno fornendo. Questo è un fatto importante per la conformità al GDPR.

Anteporre a tutto la governance dei dati

Per tutte le elaborazioni di dati che potrebbero mettere a rischio i diritti individuali, è necessario implementare un processo di valutazione dell'impatto sulla privacy (Privacy Impact Assessment, PIA). Inoltre, l'azienda deve essere in grado di spiegare le sue modalità di raccolta, utilizzo e modifica dei dati personali, e se esistono procedure implementate che consentono ai cittadini UE di fornire, rivedere e/o rifiutare con facilità i dati. Il GDPR afferma che è obbligatorio garantire che l'infrastruttura per i dati della propria società mantenga un registro di attività di elaborazione e fornisca visibilità alla conformità delle proprie pratiche.

Monitorare l’accesso ai dati di dipendenti e persone esterne

È necessario stabilire severe politiche di autorizzazione che limitino l’accesso ai dati e che garantiscano la privacy. Queste politiche devono essere aggiornate costantemente per rispecchiare le esigenze dell’azienda, controllando che vengano rispettate, specialmente per quanto riguarda il trasferimento dei dati. Nel Capitolo V del GDPR, anche le destinazioni dei trasferimenti al di fuori dell’UE devono rispettare le stesse condizioni di protezione e governance delle organizzazioni all’interno dell’UE.

I requisiti del GDPR sono severi e per essere preparati a queste normative non basta una semplice spunta delle caselle di un elenco di tutti i venditori con cui si lavora. Ma il GDPR, secondo noi, può essere un elemento utile sia per le aziende sia per i consumatori, dal momento che fornisce uniformità e certezza relativamente a privacy e protezione dei dati.

Che impatto avrà il GDPR sulle soluzioni Criteo?

Il nucleo della nostra tecnologia è rappresentato dal Criteo Shopper Graph, che riunisce i dati comportamentali dei consumatori raccolti in tutto il Criteo Commerce Marketing Ecosystem e alimenta le nostre soluzioni per il commerce marketing.

Il Criteo Shopper Graph è suddiviso in tre affidabili raccolte di dati che combinano tre tipi chiave di dati sui consumatori:

- Identificatori tecnici “pseudonimi”
- Interessi dei nostri clienti per il prodotto e per i servizi
- Statistiche di misurazione sulla performance dei nostri servizi

Verifichiamo costantemente che questi dati abbiano un utilizzo limitato a ciò che è strettamente necessario per i nostri servizi, per offrire ai consumatori informazioni rilevanti sui prodotti che desiderano, al momento giusto e con i messaggi giusti. Ad esempio:

- Criteo utilizza gli ultimissimi algoritmi di criptazione per garantire che nessun dato direttamente identificativo del consumatore venga memorizzato nei nostri sistemi.
- Non memorizziamo mai dati per un periodo più lungo di quello strettamente necessario e rispettiamo le raccomandazioni delle Autorità Europee per la Protezione dei Dati sui cookie e sulla pubblicità digitale.
- Forniamo semplici meccanismi di scelta: tutti i prodotti Criteo hanno lo stesso semplice processo di ritiro del consenso in tutti i nostri annunci e nella nostra politica sulla privacy. Siamo anche soci registrati delle seguenti piattaforme di ritiro del consenso che permettono ai clienti di opporsi alla pubblicità mirata.
- I consumatori possono rinunciare esplicitamente al servizio di Criteo facendo clic sul link Ad Choices dell’annuncio, e possono sapere perché stanno visualizzando la pubblicità. Quando un utente rinuncia esplicitamente ai servizi di Criteo, tutte le

informazioni raccolte saranno cancellate o rese irreperibili, inclusi eventuali dati utenti inseriti come parte di una campagna prodotti di Criteo.

Conclusione

Mentre le aziende del marketing digitale aggiornano le proprie pratiche per adeguarsi al GDPR, è importante ricordare che i cittadini UE sono consapevoli della pubblicità mirata, conoscono gli identificatori che la guidano e si aspettano di vedere annunci pertinenti. Criteo ha collaborato con IPSOS[4] per condurre un sondaggio sui consumatori allo scopo di comprendere quali sono le aspettative degli utenti UE e quale rapporto hanno con la pubblicità mirata online. Abbiamo intervistato 3.000 utenti Internet, di età compresa tra i 16 e i 65 anni in Francia, Regno Unito e Spagna, ritagliando un campione demografico rappresentativo per quanto riguarda genere, età, regione e livello di reddito.

Nello specifico, abbiamo scoperto che:

- Il 90% di utenti Internet è consapevole del retargeting comportamentale
- Il 68% è consapevole del fatto che i cookie consentono la pubblicità mirata
- Il 75% si aspetta di ricevere annunci adatti ai propri interessi
- I 73% preferisce vedere annunci pertinenti piuttosto che spendere di più per evitare di vedere gli annunci.

Criteo è convinta che la protezione della privacy dei consumatori, la chiarezza e la trasparenza delle pratiche commerciali siano di primaria importanza per tutti. Quando i clienti comprendono esattamente in che modo vengono utilizzati i loro dati e quando hanno il controllo delle loro informazioni personali di navigazione, la loro fiducia e la loro fedeltà in un'azienda ne vengono rafforzate.

Noi siamo pienamente consapevoli e preparati sulle implicazioni del GDPR ed è nostra ferma volontà aiutare i clienti e i partner a capire i nostri prodotti e servizi. Se collaboriamo con lo scopo di comprendere le normative e prepararci ad esse, saremo come sempre preparati per la nostra attività.

[4] *Criteo-IPSOS Study, 2017*