

PERCORSO DI FORMAZIONE PROFESSIONALE

Media Buyer

Dispensa 11 · Privacy e Compliance

A cura di Marco Consiglio

Edizione aggiornata 2026

“Il GDPR non è un ostacolo burocratico al media buying: ne definisce le regole del gioco, proprio come le regole di un'asta definiscono come si acquista uno spazio pubblicitario.”
— Marco Consiglio

Indice della dispensa

1. Introduzione e obiettivi didattici
2. Il GDPR e i principi fondamentali del trattamento dati
3. Basi giuridiche del trattamento in ambito pubblicitario
4. Cookie, consenso e il Transparency and Consent Framework
5. Il declino dei cookie di terze parti: stato dell'arte 2026
6. Consent Mode e la misurazione in assenza di consenso
7. Il Digital Services Act e la trasparenza pubblicitaria
8. Dati sensibili e categorie particolari nella pubblicità
9. Data Processing Agreement e responsabilità del media buyer
10. Costruire una strategia privacy-first
11. Caso pratico guidato
12. Glossario tecnico
13. Checklist di autoverifica
14. Riferimenti normativi e bibliografici (2026)

1. Introduzione e obiettivi didattici

Nel corso delle dispense precedenti abbiamo più volte richiamato, senza approfondirli sistematicamente, i vincoli normativi che regolano il trattamento dei dati personali nella pubblicità digitale. Questa dispensa affronta in modo organico il tema della privacy e della compliance, un ambito che negli ultimi anni ha assunto un ruolo sempre più centrale nella professione del media buyer, al punto da influenzare direttamente le scelte tecniche e strategiche trattate in tutte le dispense precedenti.

Questa dispensa non richiede conoscenze giuridiche pregresse, ma presuppone familiarità con i concetti tecnici già introdotti, in particolare Pixel, custom audience e cookie di terze parti, discussi rispettivamente nelle Dispense 3, 6 e 10.

Obiettivi didattici

1. Comprendere i principi fondamentali del GDPR applicati alla pubblicità digitale.
2. Distinguere le basi giuridiche disponibili per il trattamento dei dati in ambito pubblicitario.
3. Comprendere il funzionamento dei cookie e del Transparency and Consent Framework.
4. Conoscere lo stato dell'arte del declino dei cookie di terze parti.
5. Comprendere il funzionamento del Consent Mode e la sua importanza operativa.
6. Conoscere gli obblighi di trasparenza introdotti dal Digital Services Act.
7. Riconoscere i vincoli specifici legati al trattamento di dati sensibili.
8. Comprendere le responsabilità del media buyer nella filiera del trattamento dati.
9. Costruire una strategia pubblicitaria coerente con un approccio privacy-first.

IN SINTESI

- La privacy non è un vincolo esterno al media buying, ma un elemento strutturale della professione.
- Il quadro normativo europeo, GDPR in primis, definisce condizioni precise per ogni forma di trattamento dati pubblicitario.
- Un approccio privacy-first è oggi un vantaggio competitivo, non solo un obbligo di conformità.

2. Il GDPR e i principi fondamentali del trattamento dati

Il Regolamento Generale sulla Protezione dei Dati (GDPR), in vigore dal 2018, rappresenta il quadro normativo di riferimento per il trattamento dei dati personali in ambito europeo, e si applica a qualsiasi trattamento riguardante cittadini dell'Unione Europea, indipendentemente da dove abbia sede l'azienda che tratta i dati.

I principi cardine applicabili alla pubblicità

- Liceità, correttezza e trasparenza: ogni trattamento deve avere una base giuridica valida ed essere comunicato chiaramente all'utente.
- Limitazione della finalità: i dati raccolti per uno scopo specifico (ad esempio, l'evasione di un ordine) non possono essere automaticamente riutilizzati per finalità pubblicitarie senza un'adeguata base giuridica.
- Minimizzazione dei dati: si devono raccogliere solo i dati strettamente necessari alla finalità dichiarata, non il massimo possibile "per sicurezza".
- Limitazione della conservazione: i dati non possono essere conservati indefinitamente, ma solo per il tempo necessario alla finalità del trattamento.

Perché questi principi riguardano direttamente il media buyer

Come emerso nelle dispense precedenti a proposito di custom audience e Pixel, il media buyer tratta quotidianamente dati personali degli utenti, anche quando questi dati sono gestiti tecnicamente dalla piattaforma pubblicitaria. Questo lo rende, insieme al cliente o all'organizzazione per cui opera, corresponsabile del rispetto di questi principi, non un semplice esecutore tecnico estraneo alle implicazioni normative delle proprie scelte operative.

Un errore concettuale diffuso, specialmente tra chi si avvicina per la prima volta a questi temi, consiste nel ritenere che la responsabilità normativa ricada esclusivamente sulla piattaforma pubblicitaria utilizzata (Meta, Google, TikTok) o sul cliente proprietario dei dati, escludendo il media buyer da ogni forma di responsabilità diretta. Nella pratica, come vedremo più diffusamente nella Sezione 9, la normativa individua ruoli e responsabilità specifiche anche per chi tratta i dati operativamente per conto di terzi, anche quando non ne è il proprietario originario.

“Il GDPR non è un ostacolo burocratico al media buying: ne definisce le regole del gioco, proprio come le regole di un'asta definiscono come si acquista uno spazio pubblicitario.”

— Marco Consiglio

IN SINTESI

- Il GDPR si applica a qualsiasi trattamento riguardante cittadini europei, indipendentemente dalla sede dell'azienda.
- Liceità, limitazione della finalità, minimizzazione e limitazione della conservazione sono i principi cardine.

- Il media buyer è corresponsabile del rispetto di questi principi, non un esecutore tecnico estraneo.

3. Basi giuridiche del trattamento in ambito pubblicitario

Il GDPR individua diverse basi giuridiche che rendono lecito il trattamento di dati personali. In ambito pubblicitario, le basi più rilevanti sono il consenso e il legittimo interesse, ciascuna con condizioni e ambiti di applicazione distinti.

Il consenso

Il consenso è la base giuridica più comunemente richiesta per attività di profilazione e targeting comportamentale, come discusso nella Dispensa 6. Per essere valido, il consenso deve essere libero, specifico, informato e inequivocabile: non è sufficiente un banner che imponga implicitamente l'accettazione, né una formulazione generica che non specifichi chiaramente le finalità del trattamento.

Il legittimo interesse

Il legittimo interesse può costituire una base giuridica alternativa in alcuni contesti specifici, come il retargeting verso utenti che hanno già interagito direttamente con un sito, purché l'organizzazione conduca una valutazione di bilanciamento (legitimate interest assessment) che dimostri come l'interesse dell'inserzionista non prevalga in modo sproporzionato sui diritti e le libertà dell'utente. Questa base giuridica richiede comunque la possibilità per l'utente di opporsi al trattamento in qualsiasi momento.

Altre basi giuridiche meno rilevanti in ambito pubblicitario

Il GDPR prevede ulteriori basi giuridiche — l'esecuzione di un contratto, l'adempimento di un obbligo legale, la salvaguardia di interessi vitali, l'esecuzione di un compito di interesse pubblico — che trovano applicazione più limitata nel contesto specifico della pubblicità digitale, ma che possono rilevare in situazioni particolari: ad esempio, l'invio di comunicazioni strettamente funzionali all'esecuzione di un ordine già effettuato (come una conferma di spedizione) può basarsi sull'esecuzione del contratto, distinguendosi nettamente da una comunicazione promozionale relativa a prodotti diversi, che richiederebbe invece consenso specifico.

Base giuridica	Applicazione tipica	Requisito chiave
Consenso	Profilazione, targeting comportamentale, cookie non essenziali	Libero, specifico, informato, revocabile
Legittimo interesse	Retargeting su interazioni dirette, alcune analisi statistiche	Bilanciamento documentato, diritto di opposizione

IN SINTESI

- Consenso e legittimo interesse sono le basi giuridiche più rilevanti per la pubblicità digitale.
- Il consenso deve essere libero, specifico, informato e inequivocabile per essere valido.



4. Cookie, consenso e il Transparency and Consent Framework

I cookie, e le tecnologie di tracciamento equivalenti, richiedono in ambito europeo il consenso esplicito dell'utente per finalità diverse da quelle strettamente tecniche necessarie al funzionamento del sito, come discusso nella Dispensa 6 a proposito del declino dei cookie di terze parti.

Il Transparency and Consent Framework (TCF)

Lo standard di settore per la gestione del consenso in ambito programmatico, sviluppato da IAB Europe, è il Transparency and Consent Framework: un sistema tecnico che permette di comunicare, tra publisher, SSP, DSP e Ad Exchange descritti nella Dispensa 2, le preferenze di consenso espresse da un singolo utente, evitando che ciascun attore della filiera debba richiedere il consenso separatamente.

Implicazioni pratiche per il media buyer

Un media buyer che opera in ambito programmatico dovrebbe verificare che i publisher e le piattaforme con cui collabora siano correttamente integrati con il TCF, e che le proprie campagne siano configurate per rispettare le preferenze di consenso comunicate attraverso questo framework, escludendo automaticamente dal targeting comportamentale gli utenti che non hanno prestato consenso.

Il ruolo dei Consent Management Platform (CMP)

A livello tecnico, la raccolta del consenso avviene generalmente tramite una Consent Management Platform (CMP), il software che genera il banner di consenso visualizzato dall'utente e ne comunica le scelte agli attori integrati con il TCF. La qualità e la configurazione della CMP utilizzata dal cliente incidono direttamente sulla quantità di traffico effettivamente disponibile per il targeting comportamentale: una CMP configurata in modo eccessivamente aggressivo verso il rifiuto del consenso, o con un'interfaccia poco chiara, può ridurre significativamente il tasso di consenso ottenuto rispetto a una CMP ben progettata e trasparente, con un impatto diretto sulla scala raggiungibile dalle campagne pubblicitarie del cliente.

IN SINTESI

- I cookie non essenziali richiedono consenso esplicito, distinto da quello per finalità tecniche.
- Il Transparency and Consent Framework standardizza la comunicazione del consenso lungo la filiera programmatica.
- La qualità della Consent Management Platform utilizzata incide direttamente sul tasso di consenso ottenuto.

5. Il declino dei cookie di terze parti: stato dell'arte 2026

Come introdotto nella Dispensa 6, i principali browser hanno progressivamente limitato o eliminato il supporto ai cookie di terze parti. Ad oggi, la maggior parte dei browser più diffusi blocca questi cookie per impostazione predefinita, completando un processo di transizione che ha coinvolto l'intero settore negli ultimi anni.

Le conseguenze operative per il media buyer

Questa transizione ha reso strutturalmente meno affidabile il tracciamento comportamentale cross-site tradizionale, rafforzando l'importanza dei dati di prima parte (discussi nella Dispensa 6), del tracciamento lato server (discusso nelle Dispense 3, 5 e 10) e delle soluzioni di misurazione aggregata o basate su modelli statistici, come il Media Mix Modeling introdotto nella Dispensa 10.

Le alternative tecniche emerse

- Privacy Sandbox: iniziativa che propone alternative al tracciamento individuale, basate su elaborazione aggregata direttamente nel browser.
- Clean room di dati (data clean room): ambienti sicuri che permettono di incrociare dati di prima parte tra due organizzazioni diverse senza condividere i dati grezzi sottostanti.
- Identificatori basati su consenso: sistemi che, con il consenso esplicito dell'utente, generano un identificatore condiviso tra più piattaforme per finalità pubblicitarie.

Una transizione ormai assimilata dal settore

A differenza del clima di incertezza che caratterizzava il settore alcuni anni fa, quando l'annuncio della fine dei cookie di terze parti generava previsioni allarmistiche sulla tenuta dell'intero modello di business della pubblicità digitale, l'esperienza pratica accumulata nel frattempo ha dimostrato che il settore si è progressivamente adattato: le organizzazioni che avevano investito per tempo in dati di prima parte e infrastrutture di misurazione alternative hanno attraversato la transizione con un impatto contenuto, mentre quelle che si erano affidate quasi esclusivamente al tracciamento comportamentale tradizionale hanno dovuto affrontare un percorso di adeguamento più oneroso. Questa esperienza rafforza, con il senno di poi, l'importanza di un approccio privacy-first proattivo, discusso più diffusamente nella Sezione 10, anziché puramente reattivo ai cambiamenti normativi e tecnici del settore.

IN SINTESI

- Il declino dei cookie di terze parti è ormai un processo strutturalmente completato nel 2026.
- Privacy Sandbox, clean room di dati e identificatori basati su consenso sono le principali alternative emerse.
- Le organizzazioni che avevano investito per tempo in dati di prima parte hanno attraversato la transizione con impatto contenuto.

6. Consent Mode e la misurazione in assenza di consenso

Per rispondere alla necessità di continuare a misurare le performance pubblicitarie anche in presenza di utenti che non prestano consenso al tracciamento, Google ha sviluppato il Consent Mode, uno strumento oggi ampiamente adottato anche presso piattaforme diverse da Google stessa, secondo logiche concettualmente simili.

Come funziona concettualmente

Il Consent Mode regola dinamicamente il comportamento degli strumenti di misurazione (come il Pixel discusso nella Dispensa 3) in base alle preferenze di consenso espresse dall'utente: quando il consenso non è concesso, gli strumenti di misurazione continuano a raccogliere segnali aggregati e non identificativi, che vengono successivamente utilizzati per stimare, tramite modelli statistici, il volume di conversioni realmente generato anche dagli utenti che non hanno prestato consenso, senza tracciarli individualmente.

L'importanza di una corretta implementazione

Una configurazione errata o assente del Consent Mode comporta una sottostima sistematica delle conversioni reali, con conseguenze dirette sull'ottimizzazione algoritmica delle campagne, come discusso nella Dispensa 3 a proposito dell'Event Match Quality: un algoritmo che riceve un segnale di conversioni sistematicamente sottostimato non può ottimizzare correttamente la campagna, indipendentemente dalla qualità del targeting o della creatività.

Consent Mode di base e Consent Mode avanzato

Vale la pena distinguere tra due livelli di implementazione: il Consent Mode di base, che blocca completamente l'invio di dati quando il consenso non è concesso, e il Consent Mode avanzato, che invia segnali aggregati e non identificativi (cookieless ping) anche in assenza di consenso, permettendo la modellazione statistica descritta in questa sezione. Solo la modalità avanzata consente di recuperare, tramite stima statistica, una parte significativa del volume di conversioni altrimenti perso, rendendo questa configurazione preferibile nella quasi totalità dei contesti operativi in cui la piena conformità normativa lo consenta.

IN SINTESI

- Il Consent Mode permette di stimare le conversioni anche in assenza di consenso individuale.
- Una configurazione errata comporta una sottostima sistematica delle conversioni reali.
- Il Consent Mode avanzato, con segnali aggregati, recupera una parte significativa del volume altrimenti perso.

7. Il Digital Services Act e la trasparenza pubblicitaria

Il Digital Services Act (DSA), già richiamato nelle dispense precedenti, introduce obblighi di trasparenza specifici per la pubblicità online, in particolare per le piattaforme di grandi dimensioni (Very Large Online Platforms), categoria che comprende Meta, Google e TikTok.

I principali obblighi introdotti

- Trasparenza sui parametri di targeting: gli utenti devono poter accedere a informazioni su perché stanno visualizzando una determinata inserzione.
- Divieto di pubblicità mirata basata su categorie particolari di dati (origine etnica, orientamento sessuale, convinzioni religiose, tra le altre).
- Divieto di pubblicità mirata rivolta a minori, basata su profilazione.
- Repository pubblici delle inserzioni: le grandi piattaforme devono mantenere archivi consultabili delle inserzioni pubblicate, con informazioni sul targeting utilizzato.

Implicazioni pratiche per il media buyer

Queste disposizioni impongono al media buyer una particolare attenzione quando si opera su categorie di prodotto o servizio che potrebbero, anche indirettamente, sconfinare in categorie di dati particolari: ad esempio, campagne per prodotti farmaceutici, servizi religiosi o eventi legati a specifiche comunità richiedono una valutazione attenta delle opzioni di targeting utilizzate, per evitare configurazioni che potrebbero essere interpretate come profilazione su categorie protette.

I repository pubblici come strumento di analisi competitiva

Un aspetto interessante, spesso sottovalutato, riguarda l'utilità pratica dei repository pubblici delle inserzioni introdotti dal DSA: oltre alla loro funzione di trasparenza verso gli utenti, questi archivi rappresentano anche una fonte di analisi competitiva legittima per il media buyer, che può consultarli per osservare le strategie creative e di targeting adottate da altri inserzionisti dello stesso settore, un'opportunità di ricerca di mercato che non esisteva prima dell'introduzione di questo obbligo normativo.

IN SINTESI

- Il DSA impone obblighi di trasparenza specifici alle piattaforme di grandi dimensioni.
- Vieta la pubblicità mirata su categorie particolari di dati e rivolta a minori tramite profilazione.
- I repository pubblici delle inserzioni offrono anche un'opportunità di analisi competitiva legittima.

8. Dati sensibili e categorie particolari nella pubblicità

Il GDPR individua categorie particolari di dati personali (talvolta chiamate "dati sensibili") che godono di una protezione rafforzata: dati relativi alla salute, all'orientamento sessuale, alle convinzioni religiose o politiche, all'origine etnica, all'appartenenza sindacale, ai dati genetici e biometrici.

Perché questo tema riguarda direttamente il media buying

Alcuni settori merceologici comuni nella pratica del media buying si avvicinano, anche solo indirettamente, a queste categorie: prodotti farmaceutici o parafarmaceutici, servizi di salute mentale, prodotti legati a specifiche condizioni di salute, contenuti religiosi o politici. In questi contesti, un targeting troppo specifico rischia di dedurre implicitamente informazioni sensibili sugli utenti (ad esempio, inferire una condizione di salute dal solo interesse dichiarato per un determinato prodotto), anche senza trattare esplicitamente dati classificati come sensibili.

Un principio di cautela operativa

La pratica prudente, per un media buyer che opera in questi settori, consiste nel privilegiare forme di targeting meno inferenziali (ad esempio, contestuale piuttosto che comportamentale, come discusso nella Dispensa 6) e nel consultare, nei casi dubbi, una consulenza legale specifica, poiché le implicazioni normative in questi ambiti possono variare significativamente in base al settore specifico e alla giurisdizione di riferimento.

IN SINTESI

- Le categorie particolari di dati godono di una protezione rafforzata nel GDPR.
- Alcuni settori merceologici comuni nel media buying si avvicinano, anche indirettamente, a queste categorie.
- In questi contesti è prudente privilegiare targeting meno inferenziale e consultare una consulenza legale nei casi dubbi.

9. Data Processing Agreement e responsabilità del media buyer

Quando un media buyer, o l'agenzia per cui opera, tratta dati personali per conto di un cliente — ad esempio caricando una lista clienti come custom audience, come discusso nella Dispensa 6 — si instaura una relazione di trattamento dati che il GDPR disciplina attraverso ruoli specifici: titolare del trattamento (generalmente il cliente, proprietario dei dati) e responsabile del trattamento (generalmente l'agenzia o il media buyer, che tratta i dati per conto del titolare).

Il Data Processing Agreement (DPA)

Questa relazione dovrebbe essere formalizzata attraverso un Data Processing Agreement, un accordo che definisce le responsabilità, le finalità autorizzate del trattamento, le misure di sicurezza adottate e le modalità di gestione di eventuali violazioni dei dati (data breach). L'assenza di un DPA formalizzato, pur non invalidando di per sé il trattamento, espone entrambe le parti a rischi di non conformità in caso di controllo o contestazione.

Le responsabilità pratiche del media buyer

Nella pratica quotidiana, questo si traduce in comportamenti concreti: non conservare liste clienti oltre il tempo strettamente necessario, non riutilizzare dati di un cliente per finalità diverse da quelle concordate, garantire che l'accesso ai dati sia limitato al personale effettivamente coinvolto nella gestione della campagna, ed eliminare correttamente i dati al termine della collaborazione, quando richiesto dal cliente.

Un ulteriore aspetto pratico riguarda la gestione degli strumenti terzi eventualmente utilizzati nel flusso di lavoro — fogli di calcolo condivisi, strumenti di automazione, software di reportistica — che spesso restano al di fuori del perimetro di attenzione formale ma che, trattando anch'essi dati riconducibili a persone fisiche, rientrano a pieno titolo nell'ambito di applicazione degli stessi principi di minimizzazione e limitazione della conservazione discussi nella Sezione 2. Un audit periodico di tutti gli strumenti effettivamente utilizzati nel flusso di lavoro quotidiano, non solo delle piattaforme pubblicitarie principali, è una pratica di igiene professionale che riduce sensibilmente il rischio di esposizioni normative non intenzionali.

IN SINTESI

- Titolare e responsabile del trattamento sono ruoli distinti che il GDPR disciplina con precisione.
- Il Data Processing Agreement formalizza responsabilità e finalità autorizzate del trattamento.
- Un audit periodico di tutti gli strumenti di lavoro utilizzati riduce il rischio di esposizioni normative non intenzionali.

10. Costruire una strategia privacy-first

Oltre alla semplice conformità normativa, un approccio privacy-first rappresenta oggi una scelta strategica che può generare vantaggi competitivi concreti: costruisce fiducia con gli utenti, riduce l'esposizione a rischi normativi futuri, e si allinea a un'evoluzione del settore che appare ormai strutturale e non temporanea.

Gli elementi di una strategia privacy-first

- Investimento prioritario nella raccolta di dati di prima parte, discussa nella Dispensa 6, come base più solida e meno esposta ai cambiamenti normativi.
- Trasparenza proattiva verso gli utenti sulle finalità del trattamento, oltre il minimo legale richiesto.
- Adozione tempestiva di strumenti di tracciamento lato server e Consent Mode, per mantenere una misurazione affidabile nel rispetto delle preferenze espresse.
- Formazione continua su un quadro normativo in evoluzione, come discusso più volte in questa dispensa.

Comunicare la privacy come valore, non solo come vincolo

Un ultimo elemento, spesso trascurato, riguarda il modo in cui la strategia privacy-first viene comunicata all'interno stesso del rapporto con il cliente: presentare le scelte di compliance come un mero adempimento burocratico imposto dall'esterno tende a generare resistenza, mentre inquadrarle come parte integrante di una strategia di fiducia a lungo termine con i propri utenti finali — coerente con i valori che il cliente stesso probabilmente desidera comunicare al proprio pubblico — favorisce un allineamento più solido e duraturo tra media buyer e cliente su questi temi.

“La privacy non è più il limite entro cui operare: è diventata essa stessa una leva di differenziazione competitiva.”

— Marco Consiglio

IN SINTESI

- Un approccio privacy-first genera fiducia e riduce l'esposizione a rischi normativi futuri.
- Dati di prima parte, trasparenza proattiva e tracciamento lato server sono gli elementi chiave di questo approccio.

11. Caso pratico guidato

Passo 1 — Contesto

Un'azienda che vende integratori alimentari per il benessere psicologico affida a un media buyer un budget di 4.500 euro al mese, con l'obiettivo di generare vendite online, fornendo anche una lista clienti da utilizzare come custom audience.

Passo 2 — Analisi

Il media buyer, prima di procedere, valuta che il settore si colloca in un'area potenzialmente sensibile, poiché un targeting troppo specifico basato su interessi legati a condizioni di salute mentale potrebbe implicare un'inferenza indiretta su categorie particolari di dati, come discusso nella Sezione 8.

Passo 3 — Criticità

Analizzando la lista clienti fornita dal cliente, il media buyer nota inoltre l'assenza di un Data Processing Agreement formalizzato tra l'agenzia e il cliente, e l'assenza di indicazioni chiare su come e quando questi dati siano stati raccolti, con quale consenso, e per quanto tempo debbano essere conservati.

Passo 4 — Azione correttiva

Il media buyer richiede la formalizzazione di un DPA prima di procedere al caricamento della lista clienti, verifica con il cliente le modalità di raccolta del consenso originario, e imposta la campagna privilegiando un targeting basato su interessi generali di benessere e alimentazione, evitando interessi troppo specificamente legati a diagnosi o condizioni di salute mentale, prediligendo inoltre il retargeting su visitatori del sito, basato su legittimo interesse documentato, rispetto a un targeting comportamentale più ampio e inferenziale. Spiega inoltre al cliente, con un linguaggio accessibile e privo di eccessivi tecnicismi giuridici, le ragioni concrete di ciascuna scelta, contribuendo a costruire una comprensione condivisa di questi temi piuttosto che una semplice imposizione tecnica non compresa fino in fondo.

Passo 5 — Esito

La campagna, pur con un targeting più cauto rispetto a un approccio meno attento agli aspetti di compliance, ottiene risultati solidi e sostenibili, e il cliente apprezza l'attenzione dimostrata dal media buyer verso aspetti che, in caso di contestazione, avrebbero potuto esporre l'azienda a rischi normativi significativi, consolidando un rapporto di fiducia che va oltre la sola performance della singola campagna.

IN SINTESI

- Settori a ridosso di categorie sensibili richiedono una valutazione attenta delle opzioni di targeting utilizzate.
- Un DPA formalizzato e una verifica del consenso originario sono prerequisiti prima di trattare dati di terzi.

12. Glossario tecnico

Termine	Definizione
GDPR	Regolamento Generale sulla Protezione dei Dati, quadro normativo europeo di riferimento.
Base giuridica	Il fondamento legale che rende lecito un trattamento di dati personali.
Consenso	Base giuridica che richiede una manifestazione libera, specifica, informata e inequivocabile.
Legittimo interesse	Base giuridica basata su un bilanciamento tra interesse del trattamento e diritti dell'utente.
Transparency and Consent Framework (TCF)	Standard di settore per la comunicazione del consenso in ambito programmatico.
Consent Mode	Strumento che regola la misurazione in base alle preferenze di consenso espresse dall'utente.
Digital Services Act (DSA)	Regolamento europeo che impone obblighi di trasparenza pubblicitaria alle grandi piattaforme.
Categorie particolari di dati	Dati sensibili (salute, orientamento sessuale, convinzioni religiose, tra gli altri) con protezione rafforzata.
Titolare del trattamento	Il soggetto che determina finalità e mezzi del trattamento dei dati personali.
Responsabile del trattamento	Il soggetto che tratta dati personali per conto del titolare.
Data Processing Agreement (DPA)	Accordo che formalizza responsabilità e finalità del trattamento tra titolare e responsabile.
Privacy Sandbox	Iniziativa che propone alternative al tracciamento individuale basate su elaborazione aggregata.
Data clean room	Ambiente sicuro che permette di incrociare dati di prima parte senza condividere dati grezzi.

13. Checklist finale di autoverifica

1. Sapresti elencare i principi cardine del GDPR applicabili alla pubblicità digitale?
2. Conosci la differenza tra consenso e legittimo interesse come basi giuridiche?
3. Sapresti spiegare a cosa serve il Transparency and Consent Framework?
4. Comprendi lo stato attuale del declino dei cookie di terze parti e le sue alternative?
5. Sapresti spiegare come funziona concettualmente il Consent Mode?
6. Conosci i principali obblighi introdotti dal Digital Services Act per la pubblicità?
7. Sapresti riconoscere un settore a rischio di trattamento indiretto di categorie particolari di dati?
8. Conosci la differenza tra titolare e responsabile del trattamento?

SUGGERIMENTO DI STUDIO

- Prova a identificare, per un settore a tua scelta, se e quali categorie particolari di dati potrebbero essere indirettamente coinvolte da un targeting troppo specifico.

14. Riferimenti normativi e bibliografici (aggiornati al 2026)

Riferimenti normativi

- Regolamento (UE) 2016/679 (GDPR) — quadro normativo di riferimento per il trattamento dei dati personali.
- Regolamento (UE) 2022/2065 (Digital Services Act) — obblighi di trasparenza pubblicitaria per le grandi piattaforme.
- Direttiva ePrivacy e normative nazionali di recepimento — disciplina l'uso di cookie e tecnologie di tracciamento.
- Linee guida del Garante per la protezione dei dati personali in materia di cookie, profilazione e pubblicità comportamentale.

Fonti e risorse di approfondimento

- Documentazione ufficiale di IAB Europe sul Transparency and Consent Framework.
- Centri assistenza ufficiali delle piattaforme pubblicitarie in materia di privacy e compliance.

Questi riferimenti completano e sistematizzano quelli già citati nelle dispense precedenti; in caso di dubbi specifici relativi a un cliente o a un settore particolare, resta sempre opportuno il coinvolgimento di una consulenza legale qualificata, come già indicato nella Sezione 8.

Fine della Dispensa 11 — Privacy e Compliance

Marco Consiglio — Percorso Media Buyer, edizione 2026