CONFINDUSTRIA

Le Linee guida del Garante privacy sui *tracking pixel* nelle e-mail: principali novità e indicazioni per le imprese

Nota di Aggiornamento

Ottobre 2026

Sommario

1. Premessa 2

2. Ambito di applicazione: soggetti e comunicazioni interessate 2

3. Obblighi di informativa 3

4. Consenso al tracciamento 4

5. Deroghe all'obbligo di consenso 5

6. Misure tecniche e organizzative 7

7. Indicazioni operative per le imprese 7

1. Premessa

Con il provvedimento n. 284 del 17 aprile 2026, pubblicato nella Gazzetta Ufficiale del 29 aprile 2026, il Garante per la protezione dei dati personali (di seguito, anche "**Garante privacy**" o "**Autorità**") ha adottato le *Linee guida in materia di utilizzo di tracking pixel nelle comunicazioni di posta elettronica* (di seguito, anche "**Linee guida**"), che chiariscono la disciplina applicabile a tali strumenti e individuano i principali adempimenti per le imprese. Il **termine per l'adeguamento è fissato al 29 ottobre 2026**.

Per agevolare la comprensione delle nuove indicazioni, il Garante privacy ha inoltre pubblicato, il 5 ottobre 2026, il *vademecum* *Tracking pixel nelle e-mail. Le indicazioni del Garante*, che riepiloga i principali contenuti delle Linee guida.

I *tracking pixel* sono piccoli elementi grafici, generalmente invisibili al destinatario, inseriti nel corpo delle e-mail che, attraverso il caricamento di immagini da server remoti, consentono al mittente o a soggetti terzi di acquisire informazioni sull'apertura del messaggio. A seconda della configurazione, possono essere rilevati il momento e il numero delle aperture, l'identità del destinatario e ulteriori informazioni tecniche, quali l'indirizzo IP e il dispositivo utilizzato.

Questi strumenti possono essere impiegati per diverse finalità, tra cui, la verifica della corretta ricezione delle e-mail (*deliverability*), il contrasto allo *spam*, l'individuazione di attività di *phishing* e specifiche esigenze tecniche, anche legate alla formattazione dei messaggi. Possono, inoltre, essere utilizzati per misurare l'efficacia delle comunicazioni, rilevando le aperture e le interazioni dei destinatari, e per personalizzare successive comunicazioni sulla base degli interessi rilevati.

Il tracciamento **non riguarda direttamente il contenuto delle comunicazioni, ma l'evento della loro apertura**, dal quale possono essere ricavate informazioni utili a ricostruire comportamenti, interessi e preferenze dei destinatari. La rilevazione dell'apertura, peraltro, non equivale necessariamente alla lettura effettiva del messaggio. Inoltre, **il funzionamento dei *pixel* dipende dalle impostazioni della posta elettronica**: se il caricamento delle immagini è disabilitato, il pixel non viene caricato e l'apertura del messaggio non viene rilevata.

Sotto il profilo normativo, il Garante privacy riconduce l'utilizzo dei *tracking pixel* all'art. 122 del Codice privacy, che disciplina la memorizzazione di informazioni nei dispositivi degli utenti e l'accesso a quelle già memorizzate. In particolare, ad avviso dell'Autorità, la capacità di raccogliere informazioni attraverso l'interazione con i dispositivi dei destinatari rende tali marcatori assimilabili ai *cookie* e agli altri strumenti di tracciamento.

Il loro impiego richiede quindi, come regola generale, il consenso preventivo del destinatario, salvo specifiche deroghe, ferma restando l'applicazione dei principi e degli obblighi previsti dal Regolamento (UE) 2016/679 (GDPR).

2. Ambito di applicazione: soggetti e comunicazioni interessate

Le Linee guida si rivolgono ai soggetti, pubblici e privati, che utilizzano *tracking pixel* nelle comunicazioni di posta elettronica, direttamente o attraverso fornitori di servizi tecnologici. Sono, quindi, potenzialmente interessate **tutte le imprese che si avvalgono di sistemi di invio e-mail dotati di funzionalità di tracciamento**, anche quando forniti o gestiti da soggetti esterni.

L'utilizzo dei *tracking pixel* può riguardare diverse tipologie di comunicazioni, indipendentemente dalle modalità di accesso alla posta elettronica (*webmail*, *client* o applicazioni mobili) e dal dispositivo utilizzato. L'Autorità individua, in particolare, 4 categorie:

- **Newsletter**: comunicazioni periodiche destinate alla diffusione di aggiornamenti, contenuti informativi, comunicazioni aziendali o materiali editoriali;

- **Comunicazioni commerciali e promozionali (DEM - Direct E-mail Marketing)**: messaggi finalizzati alla promozione di prodotti, servizi o iniziative commerciali;
- **E-mail transazionali e messaggi automatici**: comunicazioni generate in relazione a specifiche azioni degli utenti o al verificarsi di determinati eventi, quali conferme di registrazione, conferme d'ordine, notifiche relative a operazioni effettuate o trasmissione di credenziali temporanee;
- **E-mail di servizio**: comunicazioni funzionali a specifiche esigenze del singolo destinatario o della collettività, anche di carattere pubblicistico.

Ai fini dell'applicazione delle Linee guida, **occorre distinguere la natura della comunicazione dalle caratteristiche e dalle finalità del tracciamento**. I *tracking pixel*, infatti, possono essere utilizzati per scopi diversi, anche non coincidenti con quelli del messaggio in cui sono inseriti. Ad esempio, un'impresa può inviare ai propri clienti una comunicazione informativa relativa a un evento o a un'iniziativa aziendale e utilizzare i dati sulle aperture per individuare i destinatari maggiormente interessati, ai quali rivolgere successive iniziative commerciali. In questo caso, pur avendo la comunicazione carattere informativo, il tracciamento persegue una finalità commerciale.

Rilevano, quindi, l'effettivo utilizzo dei *tracking pixel* e le modalità con cui vengono impiegati.

Per le imprese, ciò comporta anzitutto la necessità di verificare le funzionalità di tracciamento presenti nei sistemi e nelle piattaforme utilizzati per l'invio delle e-mail. Questa verifica costituisce il punto di partenza per individuare gli interventi di adeguamento alle Linee guida e, al tempo stesso, consente di conoscere meglio gli strumenti già in uso, così da continuare a valorizzarne le potenzialità attraverso modalità di utilizzo e configurazioni conformi alle indicazioni del Garante privacy.

Quando il trattamento coinvolge più soggetti, le Linee guida richiamano, inoltre, la necessità di **definirne i rispettivi ruoli e responsabilità**, in base alle attività concretamente svolte. Tra i soggetti interessati figurano, in particolare, il mittente delle comunicazioni, i fornitori dei servizi di invio e-mail, i gestori delle liste di distribuzione, i fornitori delle tecnologie di tracciamento e i *content creator*.

La qualificazione dei rapporti deve essere effettuata caso per caso, verificando se i soggetti coinvolti operino quali responsabili del trattamento ai sensi dell'art. 28 del GDPR, contitolari ai sensi dell'art. 26 oppure titolari autonomi.

3. Obblighi di informativa

Le Linee guida attribuiscono particolare rilievo agli obblighi di informativa, tenuto conto che i *tracking pixel* sono generalmente invisibili ai destinatari delle e-mail e possono consentire la raccolta di informazioni a loro insaputa. Il Garante privacy ribadisce, pertanto, che l'utilizzo di tali strumenti deve **essere preventivamente reso noto ai destinatari, quale condizione essenziale per la liceità del tracciamento**. Inoltre, l'obbligo di informativa sussiste indipendentemente dalla base giuridica che legittima il trattamento.

Le informazioni devono essere fornite nel rispetto dei principi di correttezza e trasparenza e degli artt. 12 e seguenti del GDPR, consentendo ai destinatari di conoscere la presenza dei *tracking pixel*, le finalità del loro utilizzo e le principali caratteristiche del trattamento.

Per agevolare l'adempimento, il Garante privacy ammette il ricorso a **informative semplificate e multilivello**. Ad esempio, al momento della raccolta dell'indirizzo e-mail può essere fornita un'informazione sintetica sull'utilizzo dei marcatori, accompagnata da un collegamento a un'informativa più dettagliata, eventualmente integrata nella *cookie* policy. È possibile ricorrere anche a diversi canali informativi, utilizzati singolarmente o in combinazione tra loro, quali *pop-up*, comunicazioni video o strumenti di interazione digitale.

La scelta delle modalità più idonee è rimessa al titolare del trattamento, che, in applicazione del principio di responsabilizzazione (*accountability*), deve verificarne l'adeguatezza rispetto agli obblighi di trasparenza. In particolare, le informazioni devono risultare complete, chiare, efficaci e facilmente fruibili dai destinatari.

Per i **trattamenti già in corso**, le Linee guida consentono di integrare le informative esistenti in occasione del primo invio utile oppure del primo momento di discontinuità del rapporto con il destinatario, sia esso contrattuale, istituzionale o di servizio.

4. Consenso al tracciamento

Come anticipato, l'utilizzo dei *tracking pixel* richiede, in linea generale, il consenso preventivo, libero, specifico, informato e inequivocabile del destinatario.

Il consenso è richiesto, in particolare, quando i marcatori consentono di monitorare individualmente le aperture delle e-mail e utilizzare le informazioni raccolte per analizzare i comportamenti dei destinatari, anche al fine di valutare e migliorare l'efficacia delle campagne promozionali.

Rientrano in queste ipotesi, ad esempio, i trattamenti che permettono di modificare l'oggetto dei messaggi in funzione dei tassi di apertura, migliorarne la pertinenza o l'attrattività, adattare la frequenza degli invii all'interesse manifestato dai singoli destinatari oppure interromperli quando le ripetute mancate aperture suggeriscono uno scarso interesse.

Il consenso è necessario anche quando le informazioni sulle aperture sono utilizzate per finalità di profilazione commerciale, ricavando indicazioni presunte sui gusti, sugli interessi e sulle preferenze dei destinatari, da impiegare per personalizzare le comunicazioni successive o orientare ulteriori iniziative promozionali.

Le Linee guida precisano le modalità di acquisizione e gestione del consenso, distinguendo tra nuovi trattamenti e trattamenti già in corso.

4.1. Nuovi trattamenti

Per i nuovi trattamenti, il consenso deve essere acquisito **prima di attivare il tracciamento**, preferibilmente al momento della raccolta dell'indirizzo e-mail, fornendo ai destinatari informazioni chiare sulle relative finalità.

Per le comunicazioni commerciali e promozionali, il Garante privacy ammette, in un'ottica di semplificazione, la possibilità di raccogliere **un unico consenso per l'invio delle comunicazioni e per il relativo tracciamento**, purché l'interessato sia adeguatamente informato di entrambe le attività e la richiesta sia formulata in modo chiaro, neutro e privo di forzature. Non è, quindi, necessario acquisire due consensi distinti.

La possibilità di esprimere un consenso unico non esclude, tuttavia, il **diritto di revocarlo separatamente per il solo tracciamento, senza rinunciare alla ricezione delle comunicazioni commerciali**. Il destinatario, infatti, deve poter continuare a ricevere tali messaggi senza che ne siano monitorate le aperture.

A tal fine, il Garante privacy suggerisce, ad esempio, di inserire nelle e-mail un collegamento o un'icona, preferibilmente nel *footer* del messaggio, che conduca a un'area di gestione delle preferenze. Il destinatario potrà così scegliere se interrompere la ricezione delle comunicazioni oppure disattivare esclusivamente il monitoraggio delle aperture.

Un'impresa che avvia una *newsletter* promozionale può, ad esempio, prevedere nel modulo di iscrizione un'unica richiesta di consenso per l'invio dei messaggi e il relativo tracciamento,

assicurando successivamente al destinatario la possibilità di continuare a ricevere la *newsletter* senza che ne siano monitorate le aperture.

4.2. Trattamenti in corso

Per i trattamenti già in corso relativi all'invio di comunicazioni commerciali contenenti *tracking pixel*, il Garante privacy prevede un **regime transitorio semplificato**, volto a consentire l'adeguamento alle Linee guida senza richiedere una nuova raccolta generalizzata dei consensi.

In particolare, le imprese che già inviano legittimamente tali comunicazioni possono integrare tempestivamente l'informativa e predisporre un meccanismo chiaramente riconoscibile e facilmente accessibile per **consentire ai destinatari di rifiutare il tracciamento delle aperture senza interrompere la ricezione dei messaggi**.

Ad esempio, un'impresa che già invia *newsletter* promozionali sulla base di un valido presupposto giuridico e utilizza una piattaforma che monitora le aperture può avvalersi del regime transitorio, aggiornando l'informativa e consentendo ai destinatari di disattivare il monitoraggio, senza procedere a una nuova raccolta generalizzata dei consensi.

La semplificazione è riservata ai trattamenti già in corso ed è destinata a esaurirsi progressivamente con l'avvio di nuove attività, soggette alle regole ordinarie di acquisizione del consenso. **Non costituisce, inoltre, una sanatoria generalizzata di eventuali violazioni pregresse**.

5. Deroghe all'obbligo di consenso

L'art. 122 del Codice privacy prevede alcune deroghe all'obbligo di consenso preventivo, applicabili anche all'utilizzo dei *tracking pixel* nelle e-mail. Le Linee guida ne chiariscono le condizioni di applicazione, distinguendo 3 principali ipotesi nelle quali il tracciamento può essere effettuato senza il consenso del destinatario.

Alla base di tali deroghe vi è un bilanciamento degli interessi operato dal Garante privacy, che riconosce come, in determinate circostanze, le informazioni raccolte attraverso i marcatori possano contribuire a rendere il servizio più efficace ed efficiente, a beneficio del destinatario, sia come singolo sia quale componente di una collettività.

Ad ogni modo, la valutazione circa l'applicabilità delle deroghe ai singoli trattamenti spetta al titolare, in conformità al principio di *accountability*. Occorre, quindi, verificare che le finalità e le modalità di utilizzo dei *tracking pixel* rispondano alle casistiche indicate dal Garante privacy.

5.1. Tracciamenti per finalità statistiche anonime

Il consenso non è necessario quando i *tracking pixel* sono utilizzati per misurare la percentuale complessiva di apertura delle e-mail, anche allo scopo di migliorare la *deliverability* e contrastare lo *spam*.

La deroga presuppone che le rilevazioni siano **effettivamente anonime e non consentano di identificare o monitorare i singoli destinatari**. L'anonimizzazione deve, quindi, riguardare anche le informazioni tecniche che, eventualmente combinate con altri dati, potrebbero consentire l'identificazione del destinatario.

Al riguardo, il Garante privacy suggerisce l'utilizzo di *pixel* identici per tutti i destinatari della stessa campagna, anziché di marcatori differenziati per ciascun utente, insieme all'anonimizzazione delle ulteriori informazioni tecniche raccolte, come l'indirizzo IP e i dati relativi al programma di posta elettronica utilizzato.

Ad esempio, un'impresa che invia una *newsletter* a 5.000 clienti può rilevare la percentuale complessiva di apertura, senza identificare i singoli destinatari. La deroga non opera, invece, se i dati consentono di risalire a chi ha aperto il messaggio e di analizzarne gli interessi commerciali.

5.2. Tracciamenti per finalità di autenticazione e sicurezza

Il consenso non è richiesto quando l'impiego dei *tracking pixel* è funzionale alla sicurezza delle procedure di autenticazione o all'erogazione di servizi richiesti dagli utenti.

Il Garante privacy richiama, in particolare, le comunicazioni relative all'attivazione di un *account*, alla modifica delle *password* e all'esercizio dei diritti in materia di protezione dei dati personali, come il diritto alla portabilità.

In tali situazioni, il monitoraggio dell'apertura può contribuire a verificare che il messaggio venga consultato attraverso un dispositivo riconducibile all'utente interessato, rafforzando la sicurezza della procedura.

Ad esempio, un'impresa che gestisce un portale riservato ai propri clienti può utilizzare un *tracking pixel* nell'ambito di una procedura di recupero delle credenziali, quando la rilevazione dell'apertura su un dispositivo noto costituisce una misura effettivamente funzionale alla sicurezza dell'operazione.

La deroga non si estende, tuttavia, automaticamente a tutte le comunicazioni relative alla gestione di un *account*, ma richiede che il tracciamento risponda concretamente alle esigenze di sicurezza o di erogazione del servizio.

5.3. Tracciamenti funzionali a comunicazioni obbligatorie o di tutela dei destinatari

Il Garante privacy ammette la possibilità di utilizzare *tracking pixel* senza consenso anche nell'ambito di comunicazioni che il mittente è giuridicamente tenuto a trasmettere o che perseguono finalità di beneficio e tutela dei destinatari, individualmente o come collettività.

Tra gli esempi richiamati dalle Linee guida rientrano le comunicazioni relative a modifiche contrattuali o delle condizioni di servizio, gli avvisi per prevenire frodi e *phishing*, le notifiche di incidenti di sicurezza, le variazioni organizzative relative a eventi programmati e i promemoria riguardanti scadenze o adempimenti contrattuali e contributivi. Sono, inoltre, richiamate le informative in materia di protezione dei dati personali e le campagne informative istituzionali.

In queste ipotesi, il tracciamento deve essere funzionale a rendere più efficace la comunicazione nell'interesse del destinatario. La rilevazione delle aperture può, ad esempio, permettere al mittente di individuare i soggetti per i quali non risulta registrata l'apertura di un avviso particolarmente importante e valutare ulteriori iniziative informative.

Si pensi a un'impresa che debba comunicare ai propri clienti un problema di sicurezza relativo a un prodotto. Il monitoraggio delle aperture potrebbe consentirle di individuare i destinatari che non risultano aver aperto l'avviso e inviare loro un ulteriore messaggio, favorendo una diffusione più efficace delle informazioni necessarie alla tutela degli utenti.

Analogamente, il tracciamento può risultare funzionale alla gestione di comunicazioni urgenti relative a incidenti informatici o a modifiche contrattuali rilevanti, quando la rilevazione dell'apertura contribuisce a garantire un'informazione tempestiva e adeguata.

La natura obbligatoria o di servizio della comunicazione non è, tuttavia, di per sé sufficiente a giustificare la deroga. Occorre che l'impiego del *tracking pixel* sia effettivamente funzionale alle esigenze che legittimano l'invio e che le informazioni raccolte siano utilizzate coerentemente con tali finalità.

6. Misure tecniche e organizzative

Le Linee guida richiamano la necessità di adottare misure tecniche e organizzative idonee a garantire il rispetto delle scelte dei destinatari e a ridurre i rischi connessi al trattamento dei loro dati personali.

Un primo aspetto riguarda la **gestione del consenso e della sua revoca**. Il Garante privacy sottolinea che tutte le scelte espresse dagli interessati devono essere adeguatamente registrate, anche ai fini della dimostrazione del rispetto della normativa, secondo quanto previsto dall'art. 7, par. 1 del GDPR.

La registrazione deve riguardare anche le eventuali revoche parziali. I sistemi utilizzati, quindi, devono consentire di distinguere le preferenze relative alla ricezione delle comunicazioni da quelle riguardanti il tracciamento, assicurando che la disattivazione dei marcatori sia effettivamente applicata ai successivi invii.

Il rifiuto del tracciamento non deve, inoltre, comportare limitazioni nella fruizione del servizio, né impedire al destinatario di continuare a ricevere le comunicazioni per le quali sussista un valido presupposto giuridico.

Un secondo aspetto riguarda la **protezione dei dati fin dalla progettazione e per impostazione predefinita** (*privacy by design e by default*), mediante l'adozione di soluzioni tecniche che limitino l'esposizione delle informazioni personali e riducano il rischio di identificazione dei destinatari.

Al riguardo, il Garante privacy suggerisce l'utilizzo di identificativi non intelligibili e non sequenziali, da associare agli indirizzi e-mail mantenendo tale corrispondenza in un ambiente interno e separato della piattaforma utilizzata.

In questo modo, la rilevazione delle aperture avviene attraverso l'identificativo associato al destinatario, senza che l'indirizzo e-mail sia direttamente incluso nella richiesta tecnica generata dal caricamento del *pixel*. Tale soluzione permette di ridurre l'esposizione dei dati personali durante la trasmissione delle informazioni, senza comportarne necessariamente l'anonimizzazione, qualora resti possibile risalire al destinatario.

Si tratta di una misura esemplificativa, che non esclude l'adozione di altre soluzioni tecniche idonee a garantire un livello di protezione adeguato, tenuto conto delle caratteristiche del trattamento e dei rischi per gli interessati.

7. Indicazioni operative per le imprese

L'adeguamento alle Linee guida comporta, sul piano operativo, una serie di verifiche sui sistemi e sulle procedure utilizzati per l'invio delle comunicazioni e-mail, finalizzate a individuare gli eventuali interventi necessari per assicurare un utilizzo dei tracking pixel conforme alle indicazioni del Garante privacy.

Di seguito, alcune indicazioni operative sulle principali attività da svolgere:

1. Verifica dei sistemi e delle piattaforme utilizzati. Occorre anzitutto accertare la presenza di *tracking pixel* nelle comunicazioni inviate, comprese quelle gestite attraverso fornitori esterni.

La verifica deve riguardare le funzionalità di tracciamento eventualmente attive, le informazioni raccolte, le finalità perseguite e le modalità con cui i dati vengono utilizzati. La ricognizione, inoltre, deve comprendere le diverse tipologie di comunicazioni aziendali, dalle newsletter e dalle campagne promozionali fino ai messaggi automatici e di servizio.

È opportuno coinvolgere i fornitori tecnologici per acquisire le informazioni necessarie, anche sulle possibilità di configurazione o disattivazione dei marcatori.

2. Valutazione delle condizioni di utilizzo. Una volta individuati i trattamenti, occorre verificare quali attività di tracciamento richiedano il consenso e quali possano beneficiare delle deroghe previste dall'art. 122 del Codice privacy.

La valutazione deve riguardare le concrete finalità e modalità di impiego dei marcatori, tenendo conto delle informazioni raccolte e delle condizioni individuate dalle Linee guida. Nei casi in cui si intenda ricorrere a una deroga, è opportuno documentare le ragioni che ne giustificano l'applicazione.

3. Aggiornamento delle informative. Occorre verificare che le informative esistenti descrivano adeguatamente l'impiego dei *tracking pixel* e le relative finalità, apportando le integrazioni necessarie.

Per i nuovi trattamenti, le informazioni devono essere fornite prima dell'attivazione del tracciamento; per quelli già in corso, l'aggiornamento può avvenire attraverso il primo invio utile o in occasione del primo momento di discontinuità del rapporto con il destinatario, secondo quanto previsto dalle Linee guida.

La scelta degli strumenti informativi resta rimessa al titolare, che deve assicurarne la completezza, la chiarezza e l'effettiva accessibilità.

4. Adeguamento dei meccanismi di consenso e revoca. Per le attività soggette a consenso, occorre verificare che questo venga acquisito prima dell'attivazione del tracciamento, attraverso modalità che informino chiaramente i destinatari delle relative finalità.

Particolare attenzione deve essere riservata alla possibilità di revocare il consenso al solo tracciamento, senza rinunciare alla ricezione delle comunicazioni. A tal fine, può essere previsto un collegamento nelle e-mail che consenta di accedere a un'area dedicata alla gestione delle preferenze.

Occorre, inoltre, verificare che le piattaforme consentano di registrare le scelte dei destinatari e di darvi effettiva attuazione, anche in caso di revoca parziale, assicurando che i successivi messaggi destinati a chi ha rifiutato il tracciamento non contengano marcatori il cui utilizzo richiede il consenso.

Per le comunicazioni commerciali già in corso, occorre assicurare un meccanismo semplice, chiaramente riconoscibile e facilmente accessibile per disattivare il monitoraggio delle aperture, continuando a ricevere le e-mail.

5. Verifica delle configurazioni tecniche e delle misure di protezione dei dati. Occorre verificare, anche con il supporto dei fornitori, le modalità con cui i *tracking pixel* raccolgono e trasmettono le informazioni, con particolare attenzione ai dati che consentono di identificare i destinatari.

In particolare, va valutata l'adozione di identificativi non intelligibili e non sequenziali, mantenendo separata la corrispondenza con gli indirizzi e-mail, secondo la soluzione suggerita dalle Linee guida. Tale accorgimento permette di evitare che l'indirizzo del destinatario sia direttamente esposto nelle richieste generate dal caricamento dei marcatori, limitando la circolazione dei dati personali.

Per i tracciamenti effettuati a fini statistici anonimi, occorre verificare che le informazioni raccolte non consentano di identificare i singoli destinatari e che gli ulteriori dati tecnici, compreso l'indirizzo IP, siano adeguatamente anonimizzati.

È, inoltre, opportuno verificare che eventuali aggiornamenti delle piattaforme o modifiche delle relative configurazioni non comportino l'attivazione di ulteriori funzionalità di tracciamento senza una preventiva valutazione della loro conformità alla disciplina applicabile.

6. Aggiornamento della documentazione e dei rapporti con i fornitori. Le verifiche effettuate e gli eventuali interventi di adeguamento devono trovare riscontro, ove necessario, nella documentazione aziendale relativa alla protezione dei dati personali.

In particolare, occorre verificare se i trattamenti connessi all'utilizzo dei *tracking pixel* siano adeguatamente descritti nel registro delle attività di trattamento, con riferimento alle finalità perseguite, alle categorie di dati raccolti, ai soggetti coinvolti e ai relativi tempi di conservazione.

Nei rapporti con i fornitori dei servizi di invio e-mail e delle tecnologie di tracciamento, è necessario verificare la corretta qualificazione dei rispettivi ruoli e, ove necessario, aggiornare gli accordi contrattuali ai sensi dell'art. 28 del GDPR o, in caso di contitolarità, dell'art. 26.

È opportuno, infine, verificare che le condizioni contrattuali e le funzionalità messe a disposizione dai fornitori siano coerenti con le modalità di trattamento adottate e consentano di rispettare le prescrizioni del Garante privacy.