GDPR & e-mail Marketing

Pericolosamente insieme

GRUPPOEASYDATA

Una disposizione di legge cristallina

Le aziende possono utilizzare i dati personali a vantaggio del business, ma le organizzazioni dovranno ripensare **il motivo e il modo** in cui li gestiscono:

- Sarà necessario rivedere e aggiornare le informative sulla privacy dei **siti web;**
- Le aziende devono fare in modo che la gestione dei consensi sia sempre adeguata e funzionante;
- Il GDPR specifica precisi requisiti per il consenso di marketing.

Quando un consenso viene revocato, le attività devono cessare immediatamente.

I principi del GDPR applicati all'e-mail Marketing.

Dai principi del GDPR discendono processi e applicazioni, cioè pratiche virtuose da adottare sempre. Quella che segue è una breve **guida pratica** per essere «compliant» quando scrivi e invii e-mailing massive di carattere promozionale o informativo a clienti o potenziali.

Per essere il più possibile concreti, abbiamo scelto

- **Carla**, appassionata di cucina oltre che ottima cuoca, sempre alla ricerca di novità sui prodotti e gli stili alimentari
- **Cook & Co**, pastificio artigianale che punta tutto sulla qualità: del prodotto, ma anche delle proprie attività di marketing.

Ci aiuteranno a capire cosa fare per rispettare l'intento del legislatore quando parla di:

1. **Trasparenza**
2. **Adeguatezza**
3. **Finalità e limitazioni**
4. **Sicurezza**
5. **Accuratezza**
6. **Responsabilità**
7. **Conservazione**
8. **Cancellazione**

1 Trasparenza

- I dati personali possono essere trattati solo per scopi specifici, espliciti e legittimi;
- Le organizzazioni devono comunicare chiaramente per quali finalità raccolgono i dati personali dell'interessato.
- La dichiarazione di consenso deve essere espressa in una forma "comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e che non contenga clausole abusive".
- Il consenso deve essere liberamente ed esplicitamente espresso.
- L'interessato deve essere informato circa il suo diritto a revocare in qualsiasi momento il consenso prestato.

Cook & Co ha pubblicato un e-book sulle migliori ricette di pasta e pesce, e Carla vorrebbe scaricarlo.

Cook & Co:

- Le deve comunicare come intendono usare i suoi dati, ad esempio se li utilizzeranno per campagne di e-mail marketing, o per la profilazione;
- Fornisce un consenso per ciascuna finalità: non è possibile unire quello per le iniziative promozionali e per il trasferimento dei dati a società terze;
- Fornisce un consenso libero: la vendita online di un prodotto non può essere vincolata all'inserimento nella mailing list;
- Non può usare i consensi pre-flaggati;
- Ogni comunicazione deve contenere la funzione "disiscriviti"
- Se desidera utilizzare i dati di Carla per un'altra finalità, deve essere richiesto un nuovo consenso.

2 Adeguatezza

- Se un’azienda intende raccogliere dati personali per convertire i visitatori di un sito in potenziali clienti, dovrà richiedere soltanto i dati **rilevanti e necessari** in ordine alla finalità dichiarata.

- I dati ridondanti, che eccedono rispetto alle finalità, rappresentano un’infrazione

”

Le condizioni e le garanzie in questione possono comprendere (..) misure tecniche e organizzative intese a ridurre al minimo il trattamento dei dati personali conformemente ai principi di proporzionalità e di necessità.

Cook & Co può richiedere a Carla nome, indirizzo di e-mail o persino cosa ama cucinare . Altre informazioni non pertinenti, come il suo stato civile, o se ha figli, non potranno essere richiesti perchè considerati eccessivi.

3 Finalità e limitazioni

- Per trasferirli ad un’altra società, le aziende devono richiedere il consenso, sempre in forma esplicita.
- Per trasferirli fuori dall’UE, devono informare l’interessato e fornirgli garanzie circa l’adeguatezza del livello di protezione.

Dopo aver scaricato l’e-book, **Carla** decide di iscriversi ad un corso di cucina online organizzato da **Cook & co**, che ne delega la logisitica ad una società terza.

Cook & Co dovrà assicurarsi il consenso al trasferimento dei suoi dati, o l’azienda terza non potrà utilizzarli.

4 Sicurezza

- I dati personali devono essere conservati in modo sicuro e protetti dall'accesso non autorizzato, perdita accidentale, distruzione o alterazione

- A seconda del tipo di dati e del modo in cui vengono utilizzati, le aziende mettono in atto misure adeguate, che possono comprendere :

  - la pseudonimizzazione/cifratura
  - la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi
  - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
    una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure
    tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Ora che i dati di **Carla** sono archiviati nei sistemi di **Cook & Co**, è responsabilità dell'azienda tenerli al sicuro.

Prima ancora di raccoglierli, avrà valutato quali tipologie di dati intende trattare e si sarà assicurata, con il team IT, che le misure adottate siano in linea con gli standard del GDPR.

Questi standard dipendono dal tipo di dato e da come viene usato: per esempio, gli standard di sicurezza dovranno essere più elevati per i dati "particolari" (salute, orientamento religioso, pendenze giudiziarie).

5 Accuratezza

In qualsiasi momento le persone devono poter correggere o aggiornare i propri dati in modo semplice e veloce.

”

E’ opportuno adottare tutte le misure ragionevoli *affinché i dati personali inesatti siano rettificati o cancellati.*

Carla ha cambiato provider di posta elettronica e ha il diritto aggiornare i suoi dati nel database di **Cook & Co**, per poter ricevere le comunicazioni sul nuovo indirizzo.

6 Responsabilità

Le aziende devono dimostrare di essere GDPR compliant, ad esempio:

- aggiornano e conservano i consensi e le cancellazioni
- implementano policy di governo dei dati, relativamente alla loro raccolta e all'utilizzo
- prendono sistematicamente in considerazione l'impatto potenziale di una nuova iniziativa **prima di realizzarla** (privacy by design).

Cook & Co organizza un webinair , attraverso un fornitore esterno, e desidera invitare **Carla**.

Prima di iniziare la campagna, deve assicurarsi che il Sistema informatico sia in grado di recepire e archiviare il consenso di Carla all'utilizzo, al trattamento e alla trasmissione dei suoi dati ad una terza parte.

Il contratto con il fornitore deve prevedere apposite clausole.

7 Conservazione

”

I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento.
*Da qui **l'obbligo**, in particolare, **di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario** (…).*
*Onde assicurare che i dati personali **non siano conservati più a lungo del necessario**, il titolare del trattamento dovrebbe **stabilire un termine per la cancellazione o per la verifica periodica**.*

Il tempo di conservazione di un dato è legato alla finalità del trattamento: deve essere previsto un tempo non superiore agli scopi per i quali il dato stesso è stato raccolto e trattato.

Lo stesso dato utilizzato per differenti finalità, può avere tempi di conservazione diversi, che devono essere opportunamente gestiti.

Carla non è più cliente di **Cook & Co**. Se questa intende prolungare la conservazione dei suoi dati, deve aver messo in atto una policy specifica, che indichi per quanto tempo conserverà i dati e la giustificazione di business.
Nella definizione del periodo di conservazione dei dati, è necessario considerare eventuali obblighi derivanti da altre disposizioni di legge, ad esempio in materia fiscale.

8 Cancellazione

A fronte di una richiesta, l'azienda deve cancellare i dati personali dai propri sistemi e assicurarsi che la stessa cosa facciano eventuali terze parti cui li abbiano trasmessi, dando conferma dell'avvenuta cancellazione.

Carla richiede la cancellazione dei propri dati dal DB di **Cook & Co**, che provvede immediatamente confermando il buon esito dell'operazione.

Privacy Compliance

Ci sono anche buone notizie.

Ekko è la società del Gruppo Easydata specializzata nella consulenza e formazione in ogni ambito della privacy**,** nata per gestire gli aspetti normativi, procedurali e tecnologici legati al GDPR.
Un team di **esperti legali e specialisti in sicurezza informatica** per guidarti nel processo di adeguamento, nella tutela dei tuoi diritti e nella **costruzione di processi aziendali migliori**.