Campagne di Email Marketing conformi al GDPR

Privacy Day Forum
CNR Area della Ricerca di Pisa, 25 maggio 2023

Avv. Matteo Maria Perlini
Avvocato e Data Protection Officer

Nel 2022

85% of marketers use email marketing software to distribute content

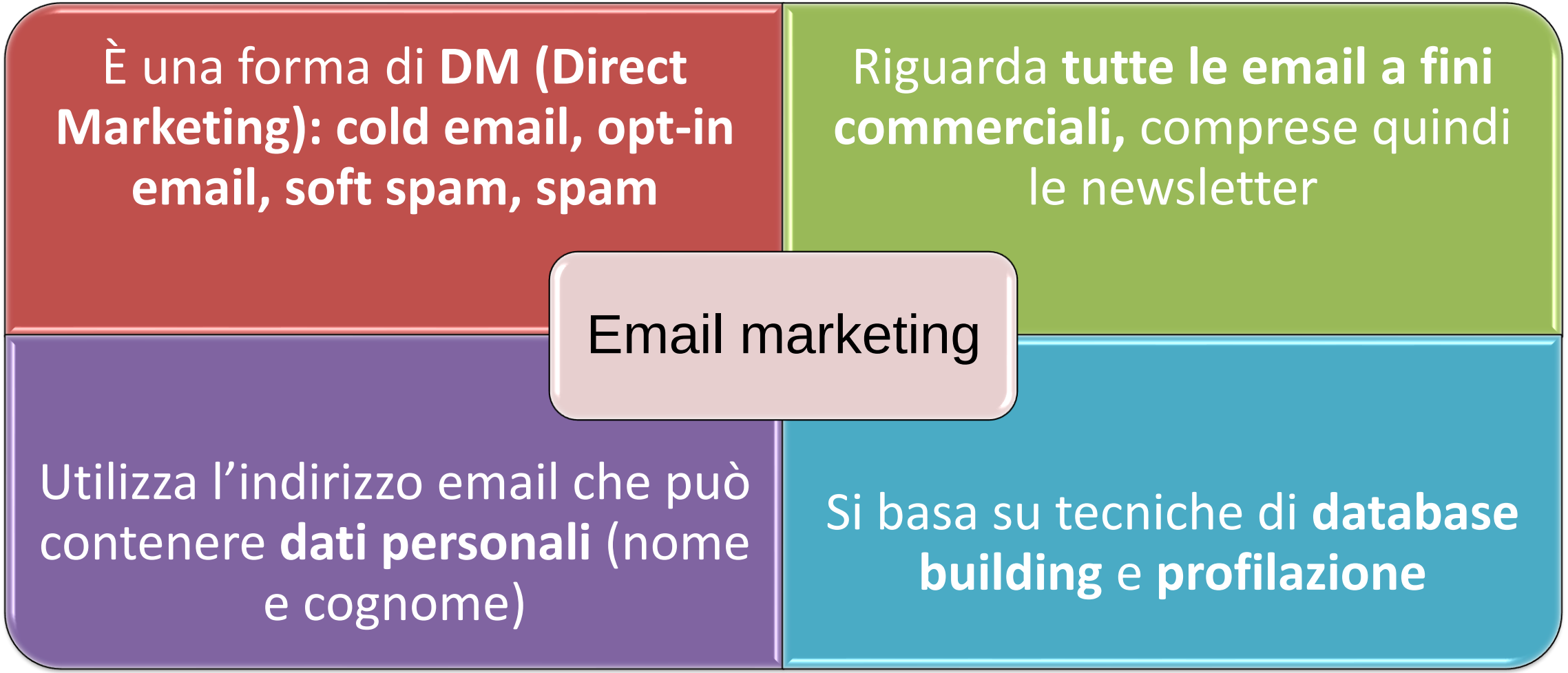
31% of them using email newsletters to nurture leads

30% of marketers use email marketing to drive conversions

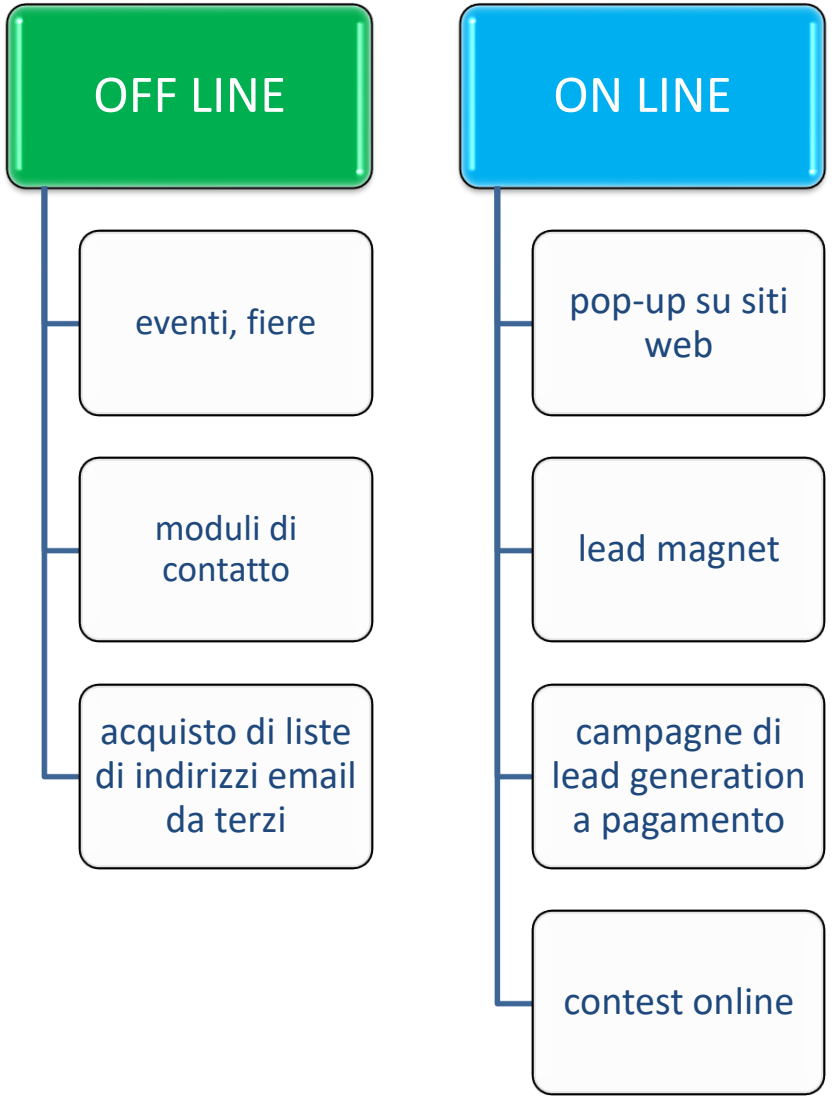
20% use it to increase customer loyalty

ActiveCampaign

Cos’è l’email marketing



Come si acquisisce un indirizzo email



L'importanza della profilazione

- Per profilazione il GDPR intende l'utilizzo di un **sistema automatizzato** attraverso cui si conoscono e si valutano gusti, interessi, abitudini degli utenti, con lo scopo appunto di inviare loro offerte commerciali personalizzate (anche utilizzando tecniche di tracciamento come il pixel tracking)
- Ma si può fare profilazione anche nei **trattamenti manuali**!

…più la profilazione è profonda, più il marketing è efficace…

Best practices ed errori da evitare

Modalità di raccolta e requisiti dei dati personali

I dati personali devono essere:

- trattati in modo lecito, corretto e trasparente (**principio di liceità, correttezza e trasparenza**);
- raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo NON incompatibile con tali finalità (**principio della limitazione della finalità**);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità (**principio della minimizzazione dei dati**);
- esatti e se necessario aggiornati (**principio di esattezza**);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**principio di limitazione della conservazione**);
- trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, con misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (**principio dell'integrità e riservatezza**).

I principi generali

Privacy by design

- valutare prima della raccolta le **finalità** per le quali i dati vengono raccolti
- valutare quali **dati** servono
- valutare le **modalità del trattamento**
- valutare il **luogo di conservazione**
- valutare il **periodo di conservazione** del dato
- valutare le **responsabilità interne**, la **catena di comando** che decide come utilizzarli e che deve rispondere di eventuali illeciti commessi
- valutare se i dati verranno trasferiti a **soggetti terzi**, quali sono questi soggetti e che garanzie danno in ottica GDPR, soprattutto se sono extra europei
- effettuare una **valutazione di impatto privacy** se necessario (profilazione)

Privacy by default

- chiedere **solo i dati strettamente indispensabili**
- impostare correttamente **form, moduli di contatto**
- predisporre **sistemi** che permettano di gestire ogni informazione in modo trasparente e che consentano la cancellazione dei dati che non sono più necessari o di gestire l'opposizione al trattamento
- predisporre **un'informativa chiara, completa, esaustiva e sempre accessibile**
- applicare una **valida base giuridica**
- formalizzare le **nomine dei fornitori**

Definire correttamente i ruoli e le responsabilità

Provv. Garante 25 novembre 2021 - doc. web n. 9737185 - caso B&T S.p.A.

*«Come meglio chiarito nelle Linee guida 7/2020 dell'EDPB, indipendentemente dalla qualificazione contrattuale dei ruoli, è **titolare** il soggetto che determina le finalità (**why**) e i mezzi, cioè le modalità (**how**), del trattamento; è invece da considerarsi responsabile il soggetto che opera **per conto** del titolare, eseguendone le istruzioni anche con un certo grado di autonomia senza tuttavia poter esercitare alcuna facoltà in ordine alla scelta delle finalità del trattamento. … **il committente di una campagna promozionale**, indipendentemente dalla materiale apprensione dei dati, deve ritenersi **titolare** del trattamento avendo in concreto determinato le decisioni in ordine alle finalità e modalità del trattamento stesso.»*

Definire correttamente i ruoli e le responsabilità

Provv. Garante 11 gennaio 2023 - doc. web n. 9861941 - caso Bakeca srl

4.3 Ruoli dei soggetti coinvolti nel trattamento

Dall'esame dei contratti forniti nel corso dell'attività ispettiva e sulla base di quanto riportato a verbale, si evince che la Società trasmette i dati dei soggetti, che hanno conferito uno specifico consenso, a terzi che utilizzano tali dati per finalità promozionali. Tali soggetti terzi, secondo la qualificazione scelta da Bakeca, in alcuni casi operano in qualità di responsabile del trattamento. Tale attribuzione dei ruoli tuttavia non risulta corretta poiché basata sull'assunto che il modello di business comunemente identificato come attività di intermediazione o di gestione/valorizzazione di data base consenta di assimilare il soggetto che si occupa di tale gestione ad un soggetto che opera per conto di Bakeca o, più specificamente, che effettua un trattamento di dati personali per conto di Bakeca. Invece, il soggetto terzo che acquisisce i dati, generalmente li utilizzerà per arricchire una propria banca dati e/o per svolgere attività promozionale per conto di propri committenti, diversi da Bakeca. Ne consegue che il rapporto che intercorre tra Bakeca e i tali partner è verosimilmente riconducibile ad un rapporto fra autonomi titolari del trattamento poiché il partner non effettua alcun trattamento per conto di Bakeca ma esegue un'attività che lo lega a Bakeca solo dal punto di vista commerciale senza tuttavia avere rilievo anche sui ruoli nel trattamento dei dati personali. Come meglio chiarito nelle Linee guida 7/2020 dell'EDPB,

Definire correttamente i ruoli e le responsabilità

Provv. Garante 23 febbraio 2023 - doc. web n. 9870014 - caso Ediscom S.p.A.

- «*il rapporto commerciale fra le parti non necessariamente ha rilievo anche sulla qualificazione dei ruoli nel trattamento* … *occorre anche ricordare che* ***non è la materiale apprensione dei dati a determinare il ruolo effettivamente svolto nel trattamento****; pertanto la Società, a seconda dell'effettiva attività svolta può qualificarsi come titolare o come responsabile ma, avendo comunque un ruolo nel trattamento, non può ritenersi un mero intermediario commerciale. Volendo semplificare, si può ritiene che essa possa agire come contitolare quando acquisisce dati, a qualsiasi titolo, da inserire nel proprio database, mentre può ritenersi responsabile del trattamento quando invece esegue attività solo per conto dei committenti ma, in tal caso, resta responsabile dei trattamenti affidati ad eventuali sub-responsabili, nei confronti del titolare (che deve previamente autorizzare per iscritto).»*

Casi pratici

1 - ***A*** *affida a* ***B*** *una ricerca di mercato relativa ai suoi prodotti istruendo B su quali informazioni raccogliere e fornendogli le domande da porre ai partecipanti.* ***A*** *riceve solo informazioni statistiche e non ha accesso ai dati personali dei partecipanti*

- **A è titolare, B è responsabile**

2 - ***A*** *e* ***B*** *lanciano un prodotto in co-branding e organizzano un evento per promuoverlo condividendo i database di clienti e potenziali clienti e stabilendo le modalità (inviti, feedback, follow-up)*

- **A** e **B** sono **contitolari**

Trasparenza

L'informativa deve essere **CHIARA, COMPLETA** ed **ESAUSTIVA**:

- **dati di contatto** del titolare del trattamento e, se nominato, del DPO
- **dati trattati**
- **finalità del trattamento** (es. invio di newsletter o analisi di mercato)
- **base giuridica** (il consenso o l'art. 130 comma 4 Codice Privacy)
- **modalità del trattamento** (scelta del target, contenuto dei messaggi, ecc.)
- **destinatari** (ciascuno dei terzi o categorie)
- **misure di sicurezza adottate** (es. crittografia del database)
- **periodo di conservazione** dei dati raccolti
- **intenzione di trasferire dati extra UE**: in particolare, servizi di terza parte utilizzati
- **diritti degli utenti** in relazione ai loro dati.

Evitare lunghi ed incomprensibili papiri!

L’informativa deve essere sempre accessibile

È necessario:

- nel **banner cookie** inserire l’informativa breve e il link all’informativa estesa;
- nelle **email di natura promozionale o newsletter** inserire il link all’informativa in calce alla email;
- all’interno dei **moduli di iscrizione** alla newsletter inserire un link alla privacy policy.

Art. 130 Codice Privacy

Comma 1: «Fermo restando quanto stabilito dagli articoli 8 e 21 del decreto legislativo 9 aprile 2003, n. 70, l'uso di **sistemi automatizzati** di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il **consenso del contraente o utente**. Resta in ogni caso fermo quanto previsto dall'articolo 1, comma 14, della legge 11 gennaio 2018, n. 5.»

La regola è l'OPT-IN anche per le persone giuridiche!

Art. 130 Codice Privacy

Il **comma 2** spiega che «La disposizione di cui al **comma 1** si applica anche alle **comunicazioni elettroniche**, effettuate per le finalità ivi indicate, mediante **posta elettronica**, telefax, messaggi del tipo MMS (Multimedia Messaging Service) o SMS (Short Message Service) o di altro tipo.»

La regola è l'OPT-IN anche per le persone giuridiche!

Requisiti del consenso

Il consenso deve essere:

- **libero**: incondizionato e senza pressioni (NO caselle preflaggate, NO consenso al marketing obbligatorio, NO dark patterns)
- **specifico**: un consenso per ogni finalità (es. un consenso per marketing, uno per profilazione, uno per la comunicazione a terzi)
- **informato**: l'interessato deve aver prima letto le informazioni necessarie (informativa)
- **inequivocabile**: attraverso un'esplicita azione affermativa
- **documentabile**: per iscritto o con tecnologie (es. registrazione di data, ora e IP di connessione al momento della compilazione della checkbox) – meglio se con **doppio opt-in**
- **revocabile**: **facilmente** (link di unsubscribe o disiscrizione in calce a ogni email che si invia) **gratuitamente** ed **in qualsiasi momento** anche ad una sola modalità di trattamento (es. email, sms)

Quando serve il consenso

- ✓ comunicazioni a **mail di proprietà di persone giuridiche**, enti o associazioni (es. amministrazione@azienda.it) ed ai **loro dipendenti**
- ✓ invio di **una prima singola comunicazione** (es. ad una persona che mi ha dato il suo biglietto da visita ad un evento)
- ✓ comunicazione ad un **lead o prospect con cui ho avuto contatti** (es. potenziale cliente che chiede informazioni o un preventivo)
- ✓ anche se **l'indirizzo mail** o il numero di cellulare **è disponibile pubblicamente** in pubblici registri o su un sito web o social network (salvo il follower che mostra inequivocabile interesse ad un prodotto)
- ✓ non solo per le comunicazioni di carattere commerciale ma anche per quelle legate a **social spam, catene di Sant'Antonio, marketing virale ed il marketing mirato**
- ✓ anche per l'invio di mail agli **indirizzi P.E.C.** contenuti nell'"indice nazionale degli indirizzi P.E.C. delle imprese e delle professioni"

Art. 130 Codice Privacy
soft spam o soft opt-in

Comma 4: si può effettuare senza consenso la vendita diretta di propri prodotti o servizi, utilizzando le **coordinate di posta elettronica fornite** dall'interessato **nel contesto della vendita di un prodotto o di un servizio**, alle seguenti condizioni:

- che si tratti di **servizi analoghi** a quelli oggetto della vendita;
- che **l'interessato, adeguatamente informato, non rifiuti tale uso**, inizialmente o in occasione di successive comunicazioni;
- che l'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata, **è informato della possibilità di opporsi in ogni momento** al trattamento, **in maniera agevole** e **gratuitamente**.

Una semplificazione

Il soft spam in dettaglio

- si applica **solo alla «posta elettronica»**;
- vale solo per la **«comunicazione commerciale»** (NO profilazione, NO cessione);
- è applicabile **solo per prodotti/servizi analoghi a quelli acquistati in passato**;
- l'**informativa** deve prevedere che sarà possibile inviare mail commerciali all'indirizzo indicato ed il **diritto di opposizione dell'interessato**;
- deve essere presente **in ogni successivo invio** la **possibilità di opporsi** ad ulteriori invii;
- deve essere **confermata la cancellazione** dal database marketing in caso di opposizione.

Per cedere banche dati

- Le società che hanno raccolto dati per finalità di marketing possono cederli ad altri soggetti che intendano utilizzarli per le stesse finalità:
  - solo dopo aver rilasciato al consumatore **un'idonea informativa** che deve indicare, oltre agli altri elementi previsti, anche **ciascuna delle terze parti** a cui i dati vengono comunicati o, in alternativa, **le categorie (economiche o merceologiche) di appartenenza** degli stessi (ad esempio: "finanza", "editoria", "abbigliamento");
  - e aver acquisito un **consenso specifico per la comunicazione (e/o cessione) a terzi** dei dati personali per fini promozionali, distinto da quello richiesto dal medesimo per svolgere esso stesso l'attività promozionale.

Per acquistare banche dati

- È necessario effettuare idonee verifiche (magari con **controlli a campione**) sui database proposti (è opportuno un contratto «blindato» con il fornitore);
- La documentazione deve recare la **data di effettuazione delle verifiche**;
- È insufficiente la documentazione del consenso con l'indicazione del solo indirizzo IP: è opportuno ad esempio **inviare un email di conferma**;
- Fornire la propria **informativa** al momento della registrazione o del primo utilizzo dei dati
- Raccogliere un **valido consenso** per l'invio di messaggi promozionali

Attenzione alle scatole cinesi!

Predisporre un registro dei consensi

Il registro dei consensi deve contenere almeno:

- **l'identità dell'utente** che ha prestato il consenso;
- a **che cosa** ha acconsentito;
- **il momento** in cui è stato prestato il consenso;
- **le informazioni** che sono state fornite all'utente nel momento in cui ha acconsentito al trattamento;
- **i metodi** utilizzati per ottenere il consenso (come un form di iscrizione alla newsletter);
- un'indicazione circa **l'eventuale revoca** del consenso.

Documentare!

Limitare la conservazione dei dati

Provv. Garante 430 del 15 dicembre 2022 docweb 9860553 – caso Assiteca:

*«**il consenso** al trattamento dei dati personali "deve ritenersi **valido**, indipendentemente dal tempo trascorso, **finché non venga revocato dall'interessato**", …ma "a condizione che sia stato correttamente acquisito in origine e che sia ancora valido alla luce delle norme applicabili al momento del trattamento nonché dei **tempi di conservazione stabiliti dal titolare**, e indicati nell'informativa"»*

Accountability!

Che orrore!

[SOSPETTO DI SPAM] ***SPAM*** Nuovo Regolamento Europeo per la protezione dei dati personali:GDPR 25.05.2018

RR Ristorante <info@ >

A m.perlini@studiolegaleperlini.it

Rispondi | Rispondi a tutti | Inoltra | ...

venerdì 31/03/2023 10:52

In caso di problemi di visualizzazione del messaggio, fare clic qui per visualizzarlo in un Web browser.

Gentile Cliente,

la tutela dei dati personali rappresenta per noi una priorità assoluta.

Per questo,Ristorante dispone di adeguate misure di sicurezza al fine di preservarne la riservatezza, l'integrità e la disponibilità.

Desideriamo informarvi che, viste le importanti novità previste dal Regolamento dell'Unione Europea n. 679/2016, noto anche come "GDPR", abbiamo aggiornato la nostra informativa sul trattamento dei tuoi dati personali.

Se vi fa piacere ricevere le nostre comunicazioni, non è necessario fare nulla, e consideriamo il silenzio assenso a continuare a ricevere le nostre comunicazioni.

Per qualsiasi ulteriore informazione contattateci a. @gmail.com

Cordiali saluti.

Ristorante

Per cancellarti da questa newsletter clicca qui

Non solo sanzioni amministrative!

- **Art. 167 comma 1 Codice Privacy**: Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sè o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e **130** o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, e' punito con la **reclusione da sei mesi a un anno e sei mesi**.

GRAZIE PER L'ATTENZIONE

✉ m.perlini@studiolegaleperlini.it

https://www.linkedin.com/in/matteo-maria-perlini-a27b2895/

https://www.studiolegaleperlini.it/professionisti/avvocato-matteo-maria-perlini/