CEIPIEMONTE S.C.P.A. | PIEMONTE AGENCY FOR INVESTMENT AND EXPORT

LA PROTEZIONE DEI DATI PERSONALI NEL SETTORE FOOD & BEVERAGE: NORMATIVA, MARKETING E CASI PARTICOLARI

Corso base in modalità webinar

Venerdì 14 aprile 2023

Docente: Ing. Monica Perego

Programma del corso

- Aspetti normativi di base
- Definizione dell'organigramma: nomina del referente privacy
- L'applicazione della Privacy by design e default e PIA
- La funzione marketing: e-commerce, termini e condizioni di servizio, siti internet, social network nel settore del Food & Beverage
- La profilazione dei clienti (b2c)
- La gestione dei profili social e degli eventi
- Scelta e valutazione dei fornitori in ottica privacy L'esercizio dei diritti da parte dei clienti

Aspetti normativi di base

- Le finalità del REG.EU 2016/679
  - I dati devono essere trattati perché producono ricchezza
  - Le condizioni affinchè possano essere trattati
    - Informativa e consenso (quando previsto)
    - Garanzia del riconoscimento dei diritti e delle libertà degli interessati
    - Applicazione delle misure tecniche ed organizzative in relazione al contesto
    - La gestione dei data breach (incidenti sulla sicurezza delle informazioni)

Definizione dell'organigramma - nomina del Referente Privacy

Le Responsabilità del Privacy Office/Referente Privacy di XXX, alle dipendenze gerarchiche del Titolare del Trattamento ed a quelle funzioni a capo del DPO (se previsto), sono le seguenti:

- *Indipendenti dalla presenza del DPO*
- *Se è stato nominato il DPO*
- *Se non è stato nominato il DPO*

Indipendenti dalla presenza del DPO

Indipendenti da presenza di DPO:

a. aggiornare le informative verso gli interessati
b. supportare le funzioni aziendali nelle nomine verso autorizzati, Responsabili esterni del trattamento, altre funzioni
c. supportare l'Amministratore di sistema nella applicazione del provvedimento a suo carico
d. supportare le funzioni aziendali nella applicazione di specifici provvedimenti emessi dal Garante
e. essere membro del Team crisi che gestisce eventuali situazioni di Data Breach
f. partecipare a riunioni ogni qualvolta si introduca all'interno dell'ente una nuova tecnologia o debbano essere attuate compagne o operazioni che riguardino il trattamento dei dati personali e impostare unitamente al Titolare del trattamento la valutazione preventiva di impatto del rischio;
g. partecipare a riunioni ogni qualvolta si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche dell'ente che impattano sulla riservatezza dei dipendenti;
h. conservare l'archivio della documentazione richiesta dal GDPR
i. supportare ufficio IT nella verifica dell'adeguatezza dei privilegi di accesso al server ed ai sistemi informatici gestionali
j. aggiungere parti di sue responsabilità sulla gestione/monitoraggio dei sistemi informatici o su gestione sue comunicazioni da e verso responsabile IT e società esterne nominate responsabili esterni del trattamento

Solo se è stato nominato il DPO

Se è stato nominato il DPO:

mettere in atto le disposizioni richieste dal DPO in materia di protezione dei dati; relazionare sullo stato di avanzamento ed eventuali problematiche

supportare il DPO nel predisporre e tenere sotto controllo il piano delle attività previste

supportare il DPO nel pianificare e condurre o sorvegliare la conduzione di attività di audit (sia di conformità al GDPR che relativi all'applicazione delle procedure interne che impattano sul GDPR); tenere sotto controllo lo stato di avanzamento delle eventuali criticità emerse nel corso dell'audit;

supportare il DPO nel tenere sotto controllo lo stato di avanzamento delle misure pianificate per la mitigazione dei rischi;

CENTRO ESTERO INTERNAZIONALIZZAZIONE
PIEMONTE Agency for Investments, Export and Tourism
Promoted by Regione Piemonte and Chambers of Commerce

Solo se non è stato nominato il DPO

Se non è stato nominato il DPO:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti; tenere aggiornato il titolare del trattamento
- supportare il Titolare del trattamento nella redazione di risposte ad hoc in caso di esercizio da parte dell'interessato dei diritti previsti a suo favore e conseguente comunicazione agli altri eventuali titolari del trattamento.
- mettere in atto le disposizione richieste dal titolare del trattamento in materia di protezione dei dati; relazionare sullo stato di avanzamento ed eventuali problematiche
- predisporre e tenere sotto controllo il piano delle attività previste in accordo con il Titolare del trattamento
- pianificare e condurre o sorvegliare la conduzione di attività di audit (sia di conformità al GDPR che relativi all'applicazione delle procedure interne che impattano sul GDPR); tenere sotto controllo lo stato di avanzamento delle eventuali criticità emerse nel corso dell'audit; tenere aggiornato il titolare del trattamento
- tenere sotto controllo lo stato di avanzamento delle misure pianificate per la mitigazione dei rischi; tenere aggiornato il titolare del trattamento
- tenere aggiornato, su indicazione del titolare del trattamento il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile ed attenendosi alle istruzioni impartite…)
- organizzare attività di formazione in materia di protezione dei dati

Definizione dell'organigramma
altre funzioni

- Il ruolo in relazione al Titolare del trattamento
- Il ruolo in relazione agli interessati
- Il ruolo in relazione al DPO – Responsabile della protezione dei dati personali e le condizioni per la sua nomina

L'applicazione della Privacy by design e default e PIA

- Privacy by design in occasione di un nuovo trattamento o modifica di un trattamento
- Esempi di nuovi trattamenti in relazione alle attività di marketing:
    - Sito di e-commerce
    - Campagna di comunicazione
    - Concorso a premi
- Privacy by default in occasione di un nuovo trattamento o modifica di un trattamento

L'applicazione della Privacy by design e default e DPIA

Elementi base della Privacy by design da considerare:

- Individuazione interessati e finalità del trattamento
- Aggiornamento del registro dei trattamenti
- Predisposizione - se necessario – di DPIA/LIA
- Valutazione adeguatezza delle misure (individuazione ed implementazione di nuove misure)
- Preparazione Informativa/consenso
- Valutazione modalità per dare corso ai diritti degli interessati
- Nomina/aggiornamento nomina dei Responsabili del trattamento
- Avvio del trattamento

La funzione marketing: e-commerce, termini e condizioni di fornitura e di servizio, siti internet, social network nel settore del Food & Beverage

- Il sito internet (di azienda/di prodotto)
- Il sito di e-commerce
  - Informativa
  - Consenso - quando richiesto….
  - Più facile…indicare quando non richiesto…
    - Esecuzione di un contratto o misure precontrattuali
    - Obbligo legale
    - Legittimo interesse del Titolare (LIA)
    - ….

La funzione marketing: e-commerce, termini e condizioni di fornitura e di servizio, siti internet, social network nel settore del Food & Beverage

Il sito di e-commerce - Condizioni di vendita

- La politica commerciale di XXX
- Come concludere il contratto col venditore
- Garanzie e indicazione dei prezzi degli articoli
- Pagamenti
- Spedizione e consegna dei prodotti
- Servizio Clienti
- Resi e Rimborsi
- Privacy
- Legge applicabile e soluzione delle controversie
- Modifica e aggiornamento
- Informazioni su XXX
- Ultimo aggiornamento del ….

www.prada.com/it/it/info/terms-conditions.html

www.armani.com/it-it/help/legalarea/saleterms

La funzione marketing: e-commerce, termini e condizioni di fornitura e di servizio, siti internet, social network nel settore del Food & Beverage

Il sito informativo - Condizioni di uso del sito

- generalità
- privacy policy
- diritti di proprietà intellettuale
- creative commons
- marchi e nomi di dominio
- links ad altri siti links ai nostri siti
- avvertenza sui contenuti
- avvertenza sul funzionamento del sito
- la nostra politica commerciale
- legge applicabile e soluzione delle controversie
- aggiornamento del documento
- ultimo aggiornamento del ….

www.prada.com/it/it/info/terms-conditions.html

www.armani.com/it-it/help/legalarea/useterms

La profilazione dei clienti (b2c)

- Il concetto di profilazione
- La profilazione manuale – effettuata con un intervento umano anche su un database
- La profilazione automatizzata – effettuata senza un intervento umano

La profilazione dei clienti (b2c)

- Le condizioni per effettuare la profilazione automatizzata rif. articolo 22 del REG. EU2 2016/679:
  - Richiesta di consenso
  - Attuazione di misure dedicate

La gestione dei profili social e degli eventi

- Evento:
  - Pubblico – non è richiesto invito
  - Privato – solo ad invito
  - Eventi particolari es. su piattaforma WEB
- Profili ed attività sui social

La gestione dei profili social e degli eventi

- Raccolta e gestione delle immagini
    - Informativa
    - Consenso
    - Liberatoria
    - Il caso dei minori

Scelta e valutazione dei fornitori in ottica privacy (es.) specifiche nel settore del Food & Beverage

- Tipologia di fornitori:
  - banche dati consenziate
  - agenzie di marketing
  - centri di contatto
  - …..

Scelta e valutazione dei fornitori in ottica privacy (es.) specifiche nel settore del Food & Beverage

- Atto di designazione:
  - Tipologia di dati trattati dal Responsabile
  - Modalità e tempi per la cancellazione/eliminazione dei dati del Titolare (versione cartacea/elettronica)
  - Criteri di scelta e qualifica di Sub-Responsabili

Scelta e valutazione dei fornitori in ottica privacy (es.) specifiche nel settore del Food & Beverage

Criteri per la qualifica iniziale generali

- posizione di leadership/monopolio sul mercato, legami ed interdipendenze con altre società leader di mercato;
- reputazione a livello nazionale/internazionale;
- certificazione del sistema di gestione qualità a fronte della UNI EN ISO 9001; essa assicura il possesso di procedure volte a dare evidenza del rispetto dei requisiti definiti contrattualmente e quindi del rispetto delle esigenze espresse dal Titolare del trattamento;
- certificazione del sistema di gestione della sicurezza delle informazioni ISO/IEC 27001; essa garantisce una serie di misure, attuate tramite controlli, sulla capacità del fornitore di garantire riservatezza, disponibilità ed integrità dell'insieme dei dati trattati per conto del cliente e considera, in caso di perdita di tali garanzie, gli impatti e le conseguenze a lungo termine sull'organizzazione;
- certificazione del sistema di gestione della sicurezza delle informazioni ISO/IEC 27701 – garantisce una serie di misure, attuate tramite controlli, sulla capacità del fornitore, in caso di perdita di riservatezza, integrità e disponibilità, di tenere sotto controllo la sicurezza dei dati personali riguardo agli impatti sugli interessati, in relazione ai loro diritti e libertà;
- altre certificazioni come ad esempio lo schema di certificazione ISDP©10003 (valutazione di conformità GDPR);
- capacità di dare riscontro a quanto previsto dal considerando 77 del GDPR, laddove recita "*…l'individuazione di migliori prassi per attenuare il rischio* [sui dati che potrebbero essere trattai dal Responsabile per conto del Titolare], *che potrebbero essere fornite in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati….";*
- esperienza specifica nel settore in cui opera il Titolare, attestata da referenze documentate; questo elemento è particolarmente qualificante nel caso in cui il Titolare operi in ambiti che presentano delle peculiarità (settore, tipo di dati trattati e/o loro quantità).

Scelta e valutazione dei fornitori in ottica privacy (es.) specifiche nel settore del Food & Beverage

Elementi di qualifica che può ottenere il Titolare in modo diretto

- raccolta di informazioni tramite questionari compilati dal potenziale fornitore (riguardanti anche le capacità tecnologiche e l'eventuale ricorso a sub-fornitori);
- documentazione a supporto della capacità, da parte del fornitore, di dare riscontro alle misure tecniche ed organizzative richieste dal Titolare del trattamento, come ad esempio esiti di test condotti da terze parti indipendenti;
- competenze specifiche e documentate del personale che verrebbe autorizzato ad operare sui dati del Titolare e, più in generale, competenze delle funzioni di staff (es. Privacy Officer) o di quelle di controllo (DPO);
- raccolta di informazioni tramite analisi di procedure (es. data breach) o altri documenti che il potenziale fornitore può rendere disponibili;
- raccolta di informazioni sulla capacità del fornitore di rispettare i KPI che il Titolare ha necessità di monitorare (es. tempi massimi di evasione di una richiesta di informazioni);
- risultanze della attività di audit di 2^ parte LINK sia sul sistema di gestione che sulla conformità legislativa, risultanze sulla base delle quali trarre conclusioni sulla capacità del potenziale fornitore di soddisfare le esigenze del Titolare;
- risultanze di uno o più incontri conoscitivi del Titolare del trattamento o suo delegato con il Referente privacy del fornitore e/o altre funzioni aziendali e/o del DPO, anche se, per quest'ultima figura, si tratterebbe di un'attività che non rientra in modo stretto tra i compiti affidati al Responsabile della protezione dei dati personali.

Scelta e valutazione dei fornitori in ottica privacy (es.) specifiche nel settore del Food & Beverage

Elementi di qualifica che può ottenere il Titolare in modo indiretto

- ricerca, su siti ed altre fonti specializzate, compreso il garante, di eventuali situazioni critiche in cui il potenziale fornitore possa essersi trovato, come ad esempio casi di data breach, provvedimenti a suo carico, ecc.;
- la presenza di un Ufficio Privacy, di un DPO e di uno staff a supporto.

Analoghe considerazioni possono essere effettuate, con i dovuti distinguo, nei seguenti casi:

- se la valutazione riguarda un potenziale Sub-Responsabile; in questo caso la qualifica è effettuata dal Responsabile e deve basarsi anche sui criteri posti dal Titolare del trattamento;
- individuazione e la scelta dei Contitolari.

Scelta e valutazione dei fornitori in ottica privacy (es.) specifiche nel settore del Food & Beverage

Criteri per la qualifica dinamica

- risultati dell'attività di audit seconda parte;
- richiesta di documentazione, come, ad esempio, i certificati di sistema di gestione/prodotto servizio e/o adesione a codici di condotta;
- risultati della ricerca su siti – ad esempio Accredia - di informazioni circa i certificati di sistema di gestione/prodotto servizio posseduti;
- capacità, documentata dal fornitore, di rispettare le misure tecniche organizzative e le istruzioni definite nell'atto di designazione del Responsabile;
- analisi delle procedure, tramesse dal Responsabile in versione aggiornata, quali data breach e quella/e previste per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative come richiede l'art. 32 par. 1d) del GDPR;
- aggiornamento delle informazioni, raccolte tramite questionari compilati dal Responsabile;
- aggiornamento delle competenze del personale (attestati/certificazioni);
- raccolta di altre evidenze di qualifica; ad esempio l'adesione al Codice CISPE "Codice di condotta per la protezione dei dati dei fornitori di servizi di infrastruttura cloud in Europa"

L'esercizio dei diritti da parte dei clienti

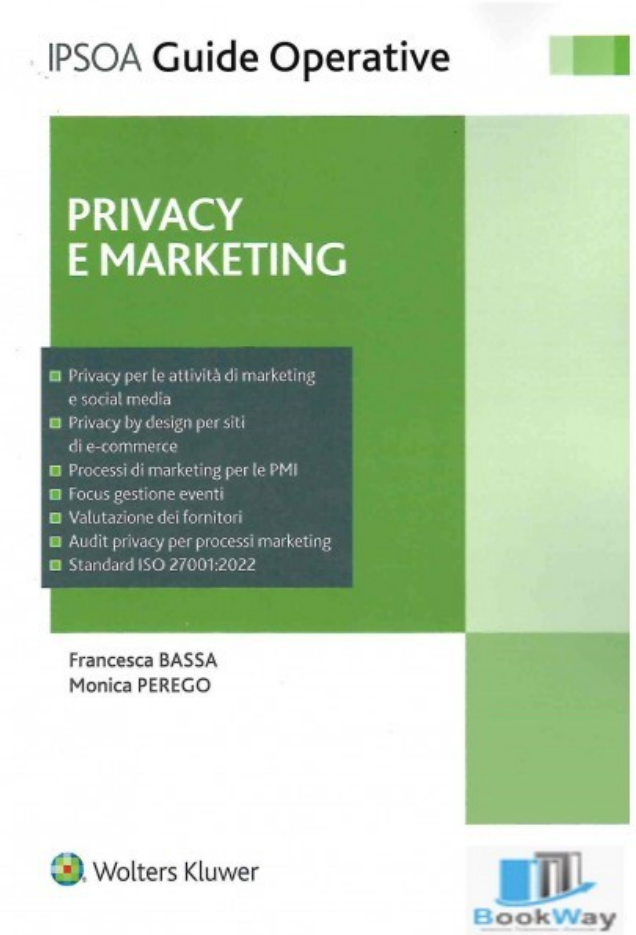
- I diritti riconosciuti rif. articoli 15÷21 del REG. EU2 2016/679
- Quali possono essere esercitati? Dipende dal contesto in cui i dati sono stati raccolti e la richiesta formulata
- Come possono essere esercitati? Attraverso una richiesta formale

L'esercizio dei diritti da parte dei clienti

I diritti dell'interessato (rif. articoli 15÷21 del REG. EU2 2016/679) possono essere esercitati, quando applicabili in qualsiasi momento e si riassumono nel diritto:

- di ottenere la conferma dell'esistenza o meno di un trattamento di dati personali che lo riguardano, e l'accesso agli stessi;
- di ottenere la rettifica dei dati senza ingiustificato ritardo, inclusa l'integrazione dei dati;
- di ottenere la cancellazione dei dati;
- di ottenere la limitazione del trattamento e la comunicazione di eventuale revoca della stessa;
- alla portabilità dei dati;
- di proporre reclamo a un'autorità di controllo.

Per approfondimenti



- Grazie!