UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

Il TRATTAMENTO DEI DATI PERSONALI NEI PROGRAMMI DI FIDELIZZAZIONE:

Il caso Douglas Italia S.p.A

Valeria Jazmin Burbano Yucailla

0348206

Anno accademico 2023/2024

INDICE

Introduzione

L’elaborato esamina l’intricato panorama del trattamento dei dati personali, un processo complesso e ampiamente regolamentato, volto a garantire la privacy degli individui e a preservare una gestione dei dati etica e trasparente. La privacy e i dati personali dei cittadini europei vengono tutelati dalla normativa dell’Unione Europea entrata in vigore il 25 maggio 2018, il Regolamento Generale sulla Protezione dei Dati (GDPR). Quest’ultimo stabilisce le rigorose linee guida per la raccolta, l'elaborazione, la conservazione e la condivisione dei dati personali, al fine di proteggere i diritti e le libertà fondamentali delle persone. Particolare attenzione verrà posta sul consenso al trattamento dei dati personali, il quale rappresenta uno dei sei presupposti legali previsti dal Regolamento Generale sulla Protezione dei Dati (GDPR). Esso costituisce un pilastro fondamentale nella tutela della privacy degli individui, assicurando che il trattamento dei loro dati avvenga esclusivamente in presenza di un consenso esplicito, informato e libero. Si esploreranno i programmi di fidelizzazione noti come fidelity card e le linee guida stabilite dal Garante per la Protezione dei Dati Personali in Italia, analizzando le modalità attraverso le quali le aziende raccolgono e gestiscono i dati.

Successivamente si procederà all’analisi di un caso di studio riguardante il provvedimento compiuto nel 2022 da parte del Garante per la protezione dei dati personali nei confronti della catena di profumerie Douglas. Questo caso illustra le violazioni riscontrate in relazione alla raccolta e gestione del consenso, le misure correttive imposte dal Garante e le implicazioni legali e aziendali del provvedimento. L'analisi del caso Douglas evidenzia le sfide che le aziende devono affrontare per conformarsi al GDPR e le conseguenze di pratiche non conformi.

1. IL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali come lo conosciamo oggi, è frutto dell'adeguamento giuridico in concomitanza dell'evolversi della società. Essi hanno duplice natura, da una parte sono attributi fondamentali della persona, dall'altra costituiscono un bene; quindi, un possibile oggetto di scambio, fonte di ricchezza e oggetto di contratto. I dati personali sono strettamente legati al diritto alla riservatezza, il quale nell'ordinamento italiano nasce in tempi recenti. Nella Costituzione Italiana del 1948 venivano considerati vari diritti fondamentali della persona, ma non quello del diritto alla riservatezza poiché non se ne sentiva la necessità. Al centro dell'ordinamento vi era il diritto alla proprietà e gli altri diritti di tipo economico.

Con il crescente sviluppo dei mezzi di diffusione di massa, quali: la radiotelevisione, la stampa e i *social media*, l'attenzione sulla tematica dei dati personali è cresciuta sempre più. I diritti della persona vengono posti al centro del sistema, cambia l'oggetto della tutela prioritaria dell'ordinamento. È l'articolo 2 della Costituzione che costituisce il riconoscimento generale della tutela della persona e dei suoi diritti fondamentali: diritto alla vita, diritto alla salute, diritto alla libertà psico-metrica, diritto alla libertà di pensiero, ecc. Il diritto alla privacy non veniva riconosciuto come diritto fondamentale della persona ma veniva tutelato indirettamente dall'articolo 2, come tutti quei diritti che sono emersi dall'evolversi della società, della sensibilità, della coscienza sociale e dall'evolversi dei costumi. Il diritto alla riservatezza nasce negli Stati Uniti nel 1980, con il saggio "*Right to Privacy*", che costituisce il diritto a non subire ingerenze non volute nella propria sfera privata.

In Italia si ha il primo riconoscimento del diritto alla riservatezza solo nel 1996 con la legge 675/1996, la prima sul trattamento dei dati personali; questa deriva dalla direttiva europea, la direttiva madre del '95. L'articolo 1 cita: "*La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione*"[1]. È la prima legge in cui vengono citati esplicitamente il diritto alla riservatezza e il diritto all'identità personale come diritto fondamentale della persona.

Si passa da diritto alla privacy quale, protezione dell'intera sfera privata di una persona da intrusioni esterne, a diritto alla riservatezza ove viene incluso il diritto al controllo dei propri dati personali. Si parla in questa fattispecie di un diritto partecipativo. A sancire il passaggio dalla concezione statica alla concezione dinamica della tutela alla riservatezza è stato il Codice della privacy, con Decreto Legislativo 196/2003), che a sua volta è stato modificato per adeguarsi al GDPR (Regolamento UE 2016/679). Quest'ultimo è entrato in vigore il 25 maggio del 2018 e il nuovo articolo 1 del Codice della privacy enuncia: "*il presente regolamento stabilisce norme relative alla protezione delle persone*

[1] Art.1, par. 1 della Legge n. 675 del 31 dicembre 1996

fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati"[2].

1.1 Regolamento Generale sulla protezione dei dati

Il Regolamento Generale sulla Protezione dei Dati (GDPR), ufficialmente noto come Regolamento (UE) 2016/679, costituisce una normativa fondamentale che ha trasformato il panorama della protezione dei dati personali in Europa. Ha lo scopo di armonizzare le leggi sulla privacy, di proteggere e responsabilizzare i cittadini dell'UE in materia di privacy dei dati e riformare il modo in cui le organizzazioni trattano i dati personali. Deve essere rispettata da tutte le organizzazioni che trattano dati personali di cittadini dell'UE, indipendentemente dal fatto che queste siano situate all'interno o all'esterno dell'Unione Europea. Vi sono dei principi fondamentali su cui si basa la normativa, e sono citati nell'articolo 5 della norma;

- Il principio di liceità, correttezza e trasparenza: i dati devono essere "*trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*"[3]. Il trattamento dei dati deve essere conforme alle norme giuridiche e il diretto interessato deve essere informato in modo chiaro sulle regole del trattamento;
- Limitazione delle finalità: i dati devono essere "*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*"[4]. Questo principio rappresenta un limite intrinseco al trattamento dei dati personali che deve avere uno scopo ben preciso;
- Minimizzazione dei dati: i dati devono essere "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*"[5]. I dati raccolti devono essere quelli strettamente necessari a perseguire la finalità prefissata e conservati per il tempo minimo necessario.
- Esattezza: i dati devono essere "*esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*"[6]. Il principio si basa sulla caratteristica di mutabilità del dato personale; di fatti, può cambiare nel corso del tempo;
- Limitazione della conservazione: i dati devono essere "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per cui sono trattati*"[7];
- Integrità e riservatezza: i dati devono essere "*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative*

[2] Art.1, par. 1 GDPR
[3] Art.5, par. 1, lett. a) GDPR
[4] Art.5, par. 1, lett. b) GDPR
[5] Art.5, par. 1, lett. c) GDPR
[6] Art.5, par. 1, lett. d) GDPR
[7] Art.5, par. 1, lett. e) GDPR

adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali"[8];

- Responsabilità (*Accountability*): il titolare del trattamento è responsabile del rispetto dei principi sopra descritti e deve essere in grado di dimostrarlo.

Inoltre, all'interno del GDPR sono presenti ulteriori articoli che definiscono i principi, i diritti e gli obblighi relativi alla protezione dei dati personali.

1.2 Il consenso al trattamento dei dati personali

Il GDPR, nell'articolo 4, fornisce definizioni essenziali che vengono utilizzate in tutto il regolamento. Queste definizioni chiariscono i termini chiave e assicurano una comprensione uniforme delle disposizioni del GDPR da parte di tutti i soggetti coinvolti. È fondamentale comprendere cosa costituisca un dato personale, ovvero qualunque informazione che riguardi una persona identificata o che consenta di identificarla, direttamente o indirettamente. Il trattamento è " *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*[9].

L'interessato è la persona a cui si riferiscono i dati personali, mentre il titolare del trattamento è colui che dirige il trattamento, determinandone le modalità e finalità.

Il consenso rappresenta la base centrale del trattamento dei dati personali e costituisce un atto positivo inequivocabile. Deve essere informato, revocabile, espresso, specifico, verificabile e libero. Il principio del consenso è strettamente legato al principio della trasparenza del trattamento, il quale "*impone che tutte le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro*"[10]. Occorre specificare che non in tutti i casi il consenso è revocabile, ad esempio quando viene dato all'interno di uno scambio negoziale, come nei servizi digitali.

Il consenso costituisce una delle sei condizioni di liceità del trattamento definite nell'articolo 6 del GDPR, dunque, non costituisce l'unica base legale del trattamento, ve ne sono altre come l'esecuzione di un contratto o il rispetto per un obbligo legale.

[8] Art.5, par. 1, lett. f) GDPR
[9] Art. 4, par. 2 GDPR
[10] Considerando n.58 GDPR

1.2 Programmi di fidelizzazione

I programmi di fidelizzazione, supportati da strumenti come le fidelity card, sono strategie di marketing che le aziende utilizzano per instaurare e mantenere relazioni a lungo termine con i consumatori. Questi programmi offrono vantaggi e incentivi ai clienti in cambio della loro fedeltà, svolgendo allo stesso la funzione di raccolta dei dati personali per ottimizzare le strategie di marketing e creare offerte personalizzate.

Gli obiettivi sono:

- Aumentare la fidelizzazione: incoraggiare i clienti a continuare ad acquistare prodotti o servizi dall'azienda;
- Raccogliere dati personali: ottenere informazioni sui comportamenti e sulle preferenze dei clienti;
- Personalizzare le offerte: utilizzare i dati raccolti per offrire promozioni e sconti personalizzati.

All'interno del contratto per l'adesione a tali programmi è presente anche la richiesta di consenso per diverse finalità quali: marketing diretto[11], profilazione e marketing da parte delle società partner. Il trattamento dei dati personali in questi contesti deve rispettare rigorosamente le normative sulla protezione dei dati.

In particolare, ai sensi dell'arti. 4 del Regolamento, si intende per profilazione "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento personale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*"[12]. Il Considerando 71 del GDPR stabilisce le linee guida per il trattamento dei dati in tale contesto:

- Deve essere basato su metodi matematici o statistici;
- Devono essere implementate decisioni che includano la verifica e la correzione dei fattori che determinano la profilazione;
- Le misure di sicurezza devono includere la crittografia, l'anonimizzazione e altri metodi per la protezione dei dati.

La profilazione richiede dunque tre caratteristiche:

- Il trattamento deve essere impiegato tramite mezzi tecnologici;

[11] Il marketing diretto è una forma di pubblicità in cui le aziende o enti comunicano direttamente con clienti specifici, anche instaurando rapporti a uno a uno. L'obiettivo è acquisire nuovi clienti, fidelizzarli e, eventualmente, recuperarli in caso di abbandono. Questo avviene attraverso l'uso di strumenti e tecniche di comunicazione che permettono di raggiungere un target definito e ottenere risposte oggettive, misurabili, quantificabili e qualificabili, migliorando così l'approccio verso i consumatori.

[12] Art. 4, par. 4 GDPR

- L'oggetto del trattamento sono i dati personali;
- Lo studio del comportamento delle persone rappresenta l'obiettivo finale della raccolta.

Qualora i dati siano raccolti personalmente presso l'interessato, il titolare del trattamento deve fornire le seguenti informazioni aggiuntive, se non già disponibili, secondo l'art. 13, "*l'esistenza di un processo decisionale automatizzato, compresa la profilazione, …, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*"[13]. Nel caso in cui i dati personali non siano stati ottenuti direttamente presso l'interessato, il titolare del trattamento deve fornire le seguenti informazioni aggiuntive secondo l'art. 14: "*l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*".[14]

Infine, la profilazione viene delineata anche negli art. 22 e 15:

- L'articolo 22 stabilisce che gli individui hanno il diritto di non essere soggetti a decisioni basate esclusivamente su trattamenti automatizzati che abbiamo effetti legali o simili significativi su di loro. L'articolo prevede delle eccezioni solo in specifici casi come il consenso esplicito dell'interessato o la necessità contrattuale, o l'autorizzazione legale, e richiede che siano messe in atto misure di salvaguardia come il diritto di intervento un intervento umano, di esprimere la propria opinione, e di contestare la decisione.
- L'articolo 15 garantisce agli individui il diritto di sapere se i loro dati personali sono oggetto di profilazione e di ottenere informazioni precise sulla modalità adottata per la profilazione. Gli interessati possono richiedere l'accesso ai dati personali trattati e alle logiche utilizzate nella profilazione, oltre a comprendere le conseguenze del trattamento, assicurando così trasparenza e controllo sui propri dati.

Il marketing diretto, nel GDPR, viene considerato come un legittimo interesse delle società; pertanto, stabilisce che questo non necessita del consenso dell'interessato, "*a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento*"[15]. Si tratta di un bilanciamento tra l'interesse legittimo della società che gestisce i dati con i diritti dell'individuo, riguardo alle comunicazioni a fini di marketing. Il più delle volte, le aziende richiedono il consenso al trattamento dei dati personali per fini promozionali non solo propri ma anche per terzi. Spesso però, non vi è una chiara delucidazione di quali siano i soggetti terzi e neanche la loro categoria merceologica di appartenenza, ciò rappresenta una violazione di quanto previsto dalla normativa privacy. Secondo il Garante, quest'ultima deve essere quantomeno specificata e i soggetti terzi devono ottenere un consenso specifico da parte dell'interessato. Solo nel caso in cui quest'ultimo abbia dato il consenso alla cessione dei suoi dati a terzi per scopi di marketing, questi possono condurre attività promozionali nei suoi confronti senza richiedere un nuovo consenso. Bisogna però

[13] Art.13, par. 2, lett. f) GDPR
[14] Art. 14, par. 2, lett. g) GDPR
[15] Considerando n.47 GDPR

specificare che in questo caso, il cessionario deve fornire un'informativa successiva all'interessato, secondo l'articolo 14 del GDPR, specificando chi ha ricevuto i dati personali.

Nel caso in cui il programma di fidelizzazione di un'azienda avvenga tramite la registrazione dei clienti tramite un'applicazione, questa dovrà rispettare le "Le linee Guida Cookie e Altri Strumenti di Tracciamento" del 10 giugno 2021, emesse dal Garante per la protezione dei dati personali, poiché vengono raccolti dati strettamente personali. Durante la navigazione all'interno dell'applicazione verranno conservate

- Informazioni sul cliente: nome, e-mail, telefono, data di nascita, sesso, ecc.;
- Attività di acquisto: Cronologia degli acquisti, prodotti acquistati, importo speso;
- Comportamento all'interno dell'app: Pagine visitate, funzionalità utilizzate, tempo trascorso, ecc.

I cookie sono file di testo di piccole dimensioni creati dai server, rappresentano gli strumenti di raccolta d'informazioni generate da un sito web e salvate dal browser dell'utente sul disco rigido locale del dispositivo utilizzato. In questo modo l'accesso ai siti web è più semplice e veloce, lo scambio di informazioni permette ai siti di riconoscere il dispositivo utilizzato e di conseguenza l'utente, in modo da inviargli informazioni personalizzate. Il passaggio di informazioni, se non consentito, viola la riservatezza degli utenti, per questo motivo la legislazione di molti Paesi, inclusa l'Italia, obbliga i siti a richiederlo esplicitamente. Ad oggi, i cookie sono considerati come dati personali e come tali vanno gestiti.

Con "Le linee Guida Cookie e Altri Strumenti di Tracciamento" del 10 giugno 2021, sono stati forniti importanti chiarimenti sulla normativa vigente, adeguandola al Regolamento. Sono stati stabiliti dei principi chiave per garantire per garantire l'uso dei cookie nel rispetto della privacy degli utenti.

1. Consenso: Gli utenti devono essere informati sull'uso dei cookie e il loro consenso deve corrispondere a un chiaro atto positivo da parte dell'utente;
2. Trasparenza: lo scopo dell'utilizzo dei cookie deve essere chiaro, così come deve essere la loro gestione;
3. Gestione delle preferenze: gli interessati devono poter esprimere le proprie preferenze riguardo ai cookie e poter revocare il consenso qualora lo desiderino;
4. Sicurezza dei dati: tutte le informazioni raccolte attraverso i cookie devono essere conservate in modo sicuro;
5. Periodicità delle informazioni: le politiche e le pratiche relative ai cookie devono essere revisionate e aggiornate.

1.3 Trattamento dei dati personali in una fusione aziendale

La fusione aziendale è un procedimento con cui due o più aziende si uniscono in una sola entità. Le norme giuridiche che regolano questo processo sono stabilite negli articoli dal 2501 al 2504-quinquies del Codice civile. Esistono due modalità principali per realizzare una fusione:

1. Fusione per unione: che comporta la creazione di una nuova società.
2. Fusione per incorporazione: dove una o più società vengono assorbite da un'altra società esistente.

La fusione può avvenire sia tra società dello stesso tipo (fusione omogenea) sia tra società di tipo diverso (fusione eterogenea). Nel caso di una fusione eterogenea, è necessaria anche la trasformazione di una o più delle società coinvolte nel processo. A queste fusioni si applicano gli stessi vincoli previsti per la trasformazione delle società. Le modalità di gestione e applicazione del GDPR in contesti di fusione vengono toccati da temi quali la compatibilità delle scelte, le questioni organizzative e quelle documentali. Tra i meccanismi oggetto delle fusioni aziendali e i beni immateriali più importanti rientrano i dati personali utilizzati dalla società target[16] per il suo business, costituiti dai database su utenti, clienti, fornitori e dipendenti. Raccogliere in modo erroneo questi dati può compromettere il valore della fusione stessa e dell'integrazione dei dati.

In caso di fusione aziendale possiede particolare rilevanza l'art. 21- Diritto di opposizione, esso stabilisce che gli interessati del trattamento dei dati possano opporsi in determinate circostanze, inclusa la fusione aziendale. Inoltre, il Considerando 48 del GDPR, perfettamente calzante nella fattispecie, enuncia: "*I titolari del trattamento che fanno parte di un gruppo imprenditoriale o di istituti affiliati a un organismo centrale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale ai fini della gestione amministrativa interna, compreso il trattamento di dati personali di clienti o dipendenti. I principi del trattamento lecito, in particolare la liceità, la correttezza e la trasparenza, il principio di limitazione della finalità, il principio di minimizzazione dei dati, il principio di esattezza, il principio di limitazione della conservazione, il principio di integrità e riservatezza e il principio di responsabilizzazione dovrebbero essere rispettati in qualsiasi trattamento di dati personali.*"[17], ammettendo il riconoscimento della trasmissione dei dati in caso di gestione amministrativa, a patto che continuino ad essere rispettati i principi del trattamento lecito dei dati.

L'introduzione del principio di accountability nel Regolamento europeo 679/2016, ha avuto un impatto significativo sulle fusioni aziendali: stabilisce che il titolare del trattamento è responsabile del rispetto delle norme e deve essere in grado di dimostrarlo attraverso misure documentabili. L'art. 24 del regolamento cita: *"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per*

[16] Azienda che subisce la fusione
[17] Considerando n.48 GDPR

garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario"[18], ciò lascia un'ampia autonomia decisionale sulla *data protection*, portando le imprese ad assumerne specificità diverse a seconda della loro organizzazione. Al momento di fusione, sia per incorporazione, che per unione, la società incorporante diverrà il nuovo titolare del trattamento dei dati e dovrà assicurare che le pratiche di protezione dei dati esistenti siano mantenute e che eventuali nuove pratiche introdotte dalla fusione siano conformi al GDPR.

Nel contesto di fusione per incorporazione, l'azienda incorporante viene chiamata *buyer* e l'azienda che subisce la fusione, *target*. La prima, antecedentemente all'operazione societaria, dovrà effettuare una *due diligence*, ossia una procedura di investigazione e di analisi per valutare gli aspetti operativi, commerciali, finanziari e operativi della seconda. In questo modo viene annullata l'asimmetria informativa verso la società target, che sarà chiamata a consegnare ogni informazione utile al buyer per avere un quadro completo dei dati personali e del loro trattamento all'interno della società.
Successivamente il buyer dovrà:

- Fornire una revisionata ed aggiornata informativa sul trattamento agli interessati, ai sensi dell'art. 14 del GDPR, soggiacendo quindi un obbligo di informativa verso gli stessi, anche nel caso in cui il trattamento dei dati fosse identico a quello precedente;
- Bilanciare gli interessi tra essa e gli interessati;
- Ottenere il consenso dell'interessato al trasferimento dei propri dati personali. In seguito, all'art. 6 del GDPR, tale consenso non risulta essere più l'elemento o il presupposto principale per il trasferimento in un contesto di fusione aziendale per varie motivazioni. La più rilevante è di carattere giuridico, avendo adempiuto ad un obbligo legale richiesto dal processo di fusione e la più pertinente è relazionata con l'art.6(1)(f): "il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali", ossia il legittimo interesse, come la continuità aziendale e l'integrazione della attività;
- Implementare, ove necessario, misure di sicurezza tecniche ed organizzative.

In caso di inadempienza di una o più di tali attività, il buyer incombe in violazioni delle prescrizioni normative del GDPR, con diverse conseguenze:

- Inutilizzabilità dei dati personali e cospicue sanzioni amministrative, è il caso in cui non è stata fornita nessuna informativa agli interessati, né verificata la sussistenza di una base giuridica. In questo caso risponde l' art.2-*decies* del Codice Privacy: "*I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*."[19] Le sanzioni sono esplicate nell'art. 83, esse sono proporzionate alla gravità della violazione e possono variare in base alla natura, alle conseguenze della violazione e alla sua durata;
- Ledere la Brand Reputation;
- Subire azioni legali: gli interessati dei dati personali possono avviare azioni legali contro la società.

[18] Art.24, par. 1 GDPR
[19] Art.2-decies DECRETO LEGISLATIVO 30 giugno 2003, n.196

2. CASO DOUGLAS ITALIA S.P.A

2.1 La nascita della Società

Douglas S.P.A. è nata in seguito all'acquisizione delle aziende Limoni, La Gardenia Beauty e Le profumerie Douglas, nel 2020, attraverso una fusione per incorporazione come parte di una strategia pianificata di espansione. Tale fusione ha rappresentato una operazione di gestione straordinaria che ha ridefinito la dimensione e la struttura organizzativa della Società. Trattandosi di una fusione per incorporazione, le società incorporate hanno cessato di esistere come entità giuridiche autonome, e i loro rapporti giuridici sono stati trasferiti alla società incorporante, come stabilito dagli articoli dal 2501 al 2505-quater della sezione II, capo X del titolo V del V del Codice civile.

Douglas è uno dei principali rivenditori di cosmetici e prodotti di bellezza in Europa. Fu fondata da Jhon Sharp Douglas nel 1821 ed iniziò con una fabbrica di saponi e profumi, evolvendosi nel tempo in un moderno business. Dopo la morte del suo fondatore, la società fu prelevata da altri investitori che mantennero il nome originale. Negli anni continuò ad evolversi, approdando nel mercato italiano nel 1989, aprì un punto vendita a Trento e a Milano. Nel 2014 Douglas si trasforma in una catena di profumerie pure-play, divenendo leader nel mercato retail europeo. Due anni dopo, nel 2016, sotto la guida del CEO Tina Muller, Douglas ha acquisito le catene italiane Limoni e La Gardenia Beauty Spa, amministrate dal gruppo Orlando Italy Management SA. Attualmente la sede legale italiane si trova a Milano e vanta oltre 500 punti vendita su tutto il territorio nazionale.

Un breve un accenno sulle società che sono state oggetto di fusione:

- La Gardenia: istituita nel 1976 dalla famiglia Croci, apre il primo negozio nel 1978. La prima grande espansione avvenne nel 1996, si ampliò in Toscana e nel Lazio, distinguendosi anch'essa per professionalità e competenza, nonché per la creazione di un ambiente esperienziale e sensorialmente piacevole. Il punto di differenziazione è sempre stato quello legato alla comunicazione, con strategie efficaci e integrate, che gli hanno permesso di rinnovarsi in modo dinamico al mercato, raggiungendo un picco di punti vendita nel 2006. Successivamente subirà l'innesto di una serie di investitori che amplieranno il mercato e il suo raggio d'azione.
- Limoni: Nasce negli anni Trenta, dalla famiglia Limoni, a Bologna, partendo come una bottega e divenuta profumeria successivamente. Negli anni '50 l'azienda attraversa una fase di sviluppo importante che dura per circa 20 anni, ritrovandosi con oltre 50 punti vendita in tutta Italia. Un passaggio importante avviene nel 2013 quando la società venne acquisita da

un investitore, la Leading Luxury Group Company, stesso acquisitore de La Gardenia, ottenendo così un controllo del 50% della distribuzione di cosmesi in Italia.

I motivi dell'acquisizione partono da un concetto semplice di Douglas, la volontà di espandersi in Europa e primeggiare in ogni mercato di competenza. Le società acquisite invece hanno commentato l'operazione come un'opportunità per soddisfare in maniera più esaustiva le esigenze dei clienti, sviluppando ulteriormente i propri business attraverso risorse finanziarie contingenti. La fusione ha portato benefici sotto vari aspetti, dalla semplificazione strutturale del gruppo, alla riduzione dei costi di gestione unificando le società, includendo una maggiore efficienza della gestione stessa, omogeneizzando le attività, rendendole efficientemente pianificate e coordinate.

Nel contesto competitivo del settore della cosmesi, in continua evoluzione, l'acquisizione di Douglas si è rivelata vantaggiosa, permettendole di soddisfare i bisogni dei consumatori sempre in costante crescita. Inoltre, la crescente difficoltà economica delle società fuse nel tentativo di sviluppare il proprio business, ha contribuito a dare un giudizio complessivo all'operazione positivo, per tutte le parti coinvolte.

2.2 Il provvedimento del Garante

2.2.1 Accertamenti ispettivi

Con il comunicato del 28 novembre 2022, in seguito alle violazioni riscontrate dal Garante Privacy, è stata resa nota la sanzione ai danni della società Douglas Italia S.p.A. La procedura era stata avviata a seguito di un reclamo risalente al 5 novembre 2020, durante l'istruttoria era stata rivelata la presenza di alcuni aspetti specifici sui trattamenti dei dati personali. Innanzitutto, era stata verificata la corretta gestione delle istanze in caso di cancellazione e opposizione al trattamento dei dati personali per motivi promozionali, con riscontro positivo. In seguito, erano stati verificati anche altri aspetti:

1. Raccolta dati mediante l'app aziendale: simulando una sottoscrizione tramite smartphone era stata rinvenuta la presenza di un'unica formula di "ok, ho capito, acconsento" come consenso per molteplici testi quali; personalizza i tuoi cookie, informativa dati personali e cookie policy, condizioni generali di vendita, di cui erano presenti i link. Questo implicava un presupposto per la violazione dell'art. 7 del Regolamento, in quanto il consenso non era reso in maniera specifica per le diverse finalità contrattuali. Inoltre, le modalità di trattamento dei dati personali in questione erano risultate prive di una base giuridica, ciò avrebbe indicato una violazione dell'art. 6.
2. Il trattamento dei dati dei clienti acquisiti dalla società precedentemente alla fusione: la società non era stata in grado di fornire le informative utilizzate separatamente dalle società Limoni Spa, La Gardenia Beauty Spa e la Profumerie Douglas Spa, questo presupponeva una violazione dell'art.5- Principio dell'Accountability;

3. Conservazione dei dati dei clienti delle singole società: era stato rilevato che i dati dei vecchi clienti, ossia quelli delle singole società prima della fusione, venivano conservati in stato inattivo nel CRM di Douglas presente sui server della società capogruppo tedesca. La società aveva dichiarato, essere 3.288.179 i vecchi clienti, sui quali non veniva effettuato nessun tipo di marketing e marketing profilato. Il motivo della conservazione era consentire un'operazione di passaggio alla nuova card Douglas più agevole, la società dichiarava inoltre: "*in ottica aziendale la società esclude dall'invio delle comunicazioni commerciali la clientela che non ha effettuato acquisti negli ultimi 24 mesi; pur rimanendo i dati (inclusi i dati relativi agli acquisti e i consensi espressi dagli interessati) all'interno del db aziendale*"[20]. La società aveva sottolineato che Douglas Italia faceva riferimento al capogruppo tedesco, il quale seguiva standard validi in tutti paesi in cui era presente la società. Anche in questo caso si era rilevata possibile la violazione dell'art. 5 in quanto la motivazione della conservazione dei dati era esclusivamente un'attuazione meramente eventuale. Inoltre, era presente un'irregolarità tra l'informativa resa ai clienti "*I dati eventualmente raccolti e trattati con il Suo consenso per le finalità indicate alle lettere e), f) e g) saranno conservati fino a che l'Interessato non revochi il consenso alla ricezione di comunicazioni commerciali da parte di Douglas o revochi il consenso all'attività di profilazione delle preferenze, o revochi il consenso alla ricezione di comunicazioni commerciali da parte dei partner di Douglas oppure richieda la cancellazione dei propri dati, salvo l'eccezionale necessità di conservare i dati per difendere i diritti di Douglas in relazione a contestazioni in essere al momento della richiesta, o su indicazione delle autorità pubbliche*"[21] e la prassi sopra citata. Questo rappresentava una possibile violazione dell'art.13;
4. Telemarketing: era stata riscontrata una discrepanza tra il modello indicato dalla capogruppo tedesca per quanto riguarda le singole modalità promozionali, sms e ricezione di telefonate da parte di un operatore, e la reale prassi operativa realizzata. Di fatti, era stato accertato che, in caso di consenso agli sms, era possibile ricevere chiamate promozionali. Questo costituiva i presupposti per la violazione dell'art. 5, 24 e 25, ovvero la non integrazione della protezione dei dati fin dalle fasi iniziali della progettazione del trattamento dei dati.

2.2.2 Difesa del titolare del trattamento

In sintesi, in base ai primi accertamenti da parte del Garante della privacy, fu contestato a Douglas, il 13 aprile 2022, la violazione dei seguenti articoli:

- Art. 5, par. 1. lett. b) ed e): del principio di accountability, di trasparenza e di limitazione della finalità;
- Art. 6: del principio di liceità per il trattamento dei dati;
- Art. 7: delle condizioni per la raccolta e l'utilizzo dei dati, il consenso deve essere specifico, libero, informato ed inequivocabile;

[20] Ordinanza ingiunzione nei confronti di Douglas Italia S.p.A
[21] Ordinanza ingiunzione nei confronti di Douglas Italia S.p.A

- Art. 13, par.2, lett. a): dell'obbligo da parte della Società di fornire informazioni chiare e trasparenti sul trattamento dei dati quando questi sono raccolti presso l'interessato, in particolare riguardo al periodo di conservazione degli stessi;
- Art. 24: della responsabilità del titolare del trattamento, egli deve essere in grado di dimostrare che le misure adottate siano conformi con il regolamento.
- Art. 25, par. 1: della *privacy by design,* l'integrazione della protezione dei dati personali fin dalle prime fasi di progettazione dei servizi e processi, e della *privacy by default*, devono essere tratti solo i dati strettamente necessari per ogni specifica finalità.

L'azienda inviò il 12 maggio 2022 una replica difensiva alle contestazioni presentate. In merito alla raccolta dei dati tramite app spiegò come la presenza dei link fosse presente per mera completezza e che con il pulsante "ok, ho capito. Acconsento" si riferisse esclusivamente all'utilizzo dei cookie. Fece sapere inoltre, che l'applicazione era in fase di aggiornamento e completamento in quanto, da ottobre 2021, la società capogruppo aveva avviato il progetto denominato "EPR Southern Europe" che si sarebbe dovuto completare ed avviare il 1° giugno 2022. Infine, indicava che il banner dei cookie sarebbe dovuto cambiare per adeguarsi alle linee guida presenti nelle "Linee guida cookie e altri strumenti di tracciamento".

Nel caso del trattamento dei dati dei clienti della società acquisite, Douglas fece sapere che prima della fusione, le relative informative delle società singole, venivano fornite ai clienti esclusivamente in store e comprendevano la sottoscrizione al programma di fidelizzazione e informativa privacy. A partire dal 2017, dalla prima operazione societaria, nei siti web di Le profumerie Douglas, Limoni e La Gardenia era presente un reindirizzamento automatico sul sito di Douglas. In questa maniera i clienti potevano iscriversi esclusivamente al programma di fidelizzazione di Douglas. Inoltre, a partire dal 2019 era entrata in atto una procedura di refresh dei consensi precedentemente ottenuti tramite l'invio della nuova informativa aggiornata. Ai clienti che non rinnovavano il consenso veniva disattivata la fidelity card e venivano dichiarati inattivi nel sistema CRM. Sugli utenti in questo stato, non veniva effettuata alcun tipo di attività di marketing, profilazione o attività da parte di terzi. In questa maniera Douglas si difese dall'aver trattato i dati dei vecchi clienti senza il loro consenso.

Per quanto riguarda l'attività di telemarketing effettuato negli store dichiara che: "*l'interessato può liberamente e specificamente esprimere separati consensi per i diversi canali di invio di comunicazioni commerciali. Il soggetto interessato, accedendo al proprio account sul sito Douglas, può selezionare e modificare i propri consensi come da schermata di seguito riportata: Tale selezione viene riflessa nel tool CRM, così come nel sistema cassa dei negozi … Le liste create per l'invio di comunicazioni di marketing vengono sempre estratte dalla Società tenendo conto dei consensi espressi dal soggetto interessato. Non sussistono, pertanto, scostamenti tra il modello adottato da Douglas e la prassi operativa. A conferma di quanto sin qui argomentato, si rileva che la Società non ha mai ricevuto contestazioni da soggetti interessati che lamentano l'improprio utilizzo dei canali marketing in violazione dei consensi dagli stessi precedentemente prestati. Quanto sopra trova altresì puntuale conferma nella dichiarazione rilasciata dal responsabile dello store di Nola …, in occasione dell'ispezione avvenuta il 16 dicembre 2021. Come infatti riferi(to) vengono effettuate "telefonate promozionali solo alle utenze presenti nelle liste di clienti VIP presenti a sistema alle quali accede tramite apposite credenziali personali. Si tratta, dunque, di un'attività di telemarketing estremamente*

ristretta e dedicata ai soli clienti definiti VIP, in base alla quale non si possono "contattare numeri di utenze telefoniche non presenti nelle liste fornite dalla società e ciò, dunque, nel pieno rispetto dei consensi liberamente espressi dai soggetti interessati"[22].

In seguito, Douglas ha chiesto l'archiviazione del procedimento amministrativo o di determinare una riduzione dell'eventuale sanzione pecuniaria applicabile.

2.2.3 Valutazioni giuridiche

Per quanto concerne il consenso al trattamento dei dati personali presente nell'app tramite il pulsante "ok, ho capito. Acconsento": nonostante siano state accettate le argomentazioni di difesa da parte di Douglas, ovvero, che il consenso riguardava esclusivamente l'utilizzo dei cookie e non altre finalità, rimaneva poco chiara la configurazione dell'applicazione. Di fatti, l'informativa conteneva specifiche per diverse finalità del trattamento dei dati, inclusa la geolocalizzazione o marketing di prossimità che Douglas aveva dichiarato di non effettuare. Il Regolamento indica come il consenso deve essere correlato ad un quadro identificativo chiaro in modo tale che vi sia condizione di liceità, accessibilità e fruibilità delle informazioni. Questo è previsto dall'art. 12, par.1 *"Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato."*[23] per tutelare il principio di trasparenza. Un aggravante era costituito dalla dichiarazione da parte di Douglas di non aver adeguato la gestione dei cookies alle indicazioni fornite dal Garante nelle "Linee guida cookie e altri strumenti di tracciamento" del 10 giugno 2021, nonostante il tempo previsto per l'adeguamento fosse di sei mesi. In seguito a queste considerazioni, era stato reso necessario confermare la violazione dell'art.5 e dell'art.12, par.1.

Riguardo le informative mancanti delle società incorporate era stato deciso di archiviare la contestazione poiché Douglas aveva fornito (anche se solo in sede di memoria) i testi, dimostrando di adempiere al principio di accountability.

L'art. 5 veniva violato anche in relazione alla conservazione dei dati personali dei clienti delle tre società incorporate, in quanto risultava eccessiva sia in termini qualitativi che temporali. In generale questa è sottoposta alla normativa in quanto costituisce un trattamento di dati personali e di conseguenza doveva rispettare le linee guida al suo interno. In particolare, il Garante aveva fornito il provvedimento "Fidelity card e garanzie per i consumatori. Le regole del garante per i programmi di fidelizzazione" del 24 febbraio 2005 in cui si stabiliva che i dati possono essere conservati per un tempo massimo di 12 o 24 mesi nel caso in cui siano utilizzati rispettivamente per scopi di marketing o profilazione. Questo limite temporale era ancora più stretto considerando il contesto di analisi, ovvero una fusione di società, in cui i vecchi clienti non aveva

[22] Ordinanza ingiunzione nei confronti di Douglas Italia S.p.A
[23] Art. 12, par.1 GDPR

rinnovato il consenso alla nuova normativa. A causa di questa violazione era stata disposta un'ingiunzione nei confronti di Douglas e imposte misure organizzative in modo tale che la conservazione avvenisse entro i limiti conformi al principio di finalità e conservazione.

Infine, per quanto riguarda il telemarketing svolto negli store, era stato rilevato che anche i clienti VIP, nonostante esprimevano il consenso esclusivamente per il contatto telefonico tramite sms, ricevevano anche chiamate telefoniche e viceversa. Venne quindi confermata la violazione degli art. 25, par. 1, art. 5, par.2 e art.24, non era stato però messo in atto alcuna prescrizione correttiva in quanto si trattava di un'attività sporadica e che la Società aveva dichiarato di aver introdotto misure che adeguavano il processo alle normative vigenti.

2.2.4 Misure da adottare

In relazione agli articoli violati, le misure da adottare furono:

- Cambiare l'impostazione dell'app Douglas;
- Separare chiaramente l'informativa sulla privacy e quella sui cookie dai termini contrattuali e dai rispettivi consensi;
- Indicare nelle informative solo i trattamenti effettivamente svolti e le finalità realmente perseguite;
- Cancellare i dati personali dei clienti delle tre società risalenti ad un massimo di 10 anni entro 30 giorni dal provvedimento, nel caso in cui questi non rinnovino la fidelity card, di cancellarli entro 15 giorni;
- Attuare misure per la conservazione dei dati in modo tale da rispettare i principi dell'art.5, soprattutto quello di finalità e minimizzazione;
- Documentazione delle misure messe in atto richieste entra 30 giorni dalla ricezione del provvedimento;
- Adottare un'ordinanza di ingiunzione per l'applicazione delle sanzioni amministrative pecuniarie previste dall'art.83, par.4 e 5, del Regolamento.

2.2.5 Sanzioni

Per l'applicazione della sanzione amministrativa si prese in considerazione l'art.83: "*Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave*"[24]. Nel caso di Douglas, la violazione più grave commessa fu quella relativa del principio di liceità indicato nell'art.6, le violazioni minori furono assorbite la quest'ultima.

[24] Art. 83, par.3 GDPR

Per determinare l'ammontare della sanzione si prese in considerazione l'art.81 par.1 e par.2, ossia essere "*effettiva, proporzionata e dissuasiva*"[25] e considerare:

- "*la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito*"[26];
- *"il carattere doloso o colposo della violazione";* [27]
- *"le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;"*[28]

Vennero anche considerate le situazioni aggravanti presenti:

- il numero elevato di violazioni di diversa natura, l'elevato numero di interessati e l'elevato intervallo di tempo per cui si era protratta la violazione;
- la rilevanza economica della società;

Presenti furono anche le attenuanti:

- l'attività di telemarking era stata di natura sporadica;
- erano in corso misure per migliorare la conformità alla normativa relativa alla protezione dati;
- non erano presenti altri procedimenti verso la Società:
- Douglas Italia aveva un limitato potere decisionale nella strategia per il trattamento dei dati personali.

In base agli elementi sopracitati e tenendo conto del bilanciamento necessario fra i diritti degli interessati e la libertà d'impresa, si applicò una sanzione amministrativa nei confronti di Douglas Italia pari a 1.400.000,00, ossia il 0,4 del suindicato fatturato. L'importo di tale sanzione venne deciso in modo tale da non recare un impatto economico troppo elevato sulle esigenze organizzative, funzionali ed occupazionali della Società.

[25] Art. 83, par. 1 GDPR
[26] Art.83, par2, lett. a) GDPR
[27] Art. 83, par.2, lett. b) GDPR
[28] Art. 83, par.2, lett. c) GDPR

Conclusioni

In conclusione, il trattamento dei dati personali rappresenta un elemento centrale per la tutela della privacy degli individui, un aspetto che assume un'importanza ancora maggiore nel contesto commerciale dei programmi di fidelizzazione e nell'uso delle app e degli store fisici. La presente analisi ha messo in luce le complessità e le sfide che le aziende devono affrontare per garantire il rispetto delle normative vigenti, evidenziando come un approccio proattivo e conforme possa non solo evitare sanzioni, ma anche costruire un rapporto di fiducia duraturo con i clienti. I programmi di fidelizzazione offrono vantaggi significativi, sia per le aziende, che possono migliorare la personalizzazione delle offerte e quindi aumentare la fedeltà dei clienti, sia per i consumatori, che beneficiano di promozioni e servizi su misura. Tuttavia, per sfruttare appieno questi benefici, è essenziale che il consenso degli utenti sia ottenuto in maniera chiara, informata e specifica. Questo implica che nelle app e negli store fisici, gli utenti devono essere pienamente consapevoli di come i loro dati verranno utilizzati e devono avere la possibilità di revocare il consenso in qualsiasi momento.

Il caso di Douglas e il relativo provvedimento del Garante Privacy italiano sottolineano l'importanza di una gestione corretta e trasparente dei dati raccolti. Douglas, come molti altri attori del settore, ha dovuto confrontarsi con le conseguenze di pratiche di trattamento dei dati personali prive di una solida base giuridica. Questo caso esemplifica come la non conformità possa portare a sanzioni significative e a un danno reputazionale, mettendo in evidenza la necessità per le aziende di adottare misure rigorose per assicurare la conformità alle leggi sulla protezione dei dati. La trasparenza e la chiarezza nella raccolta e nell'uso dei dati sono fondamentali per mantenere la fiducia dei consumatori. Le informative sulla privacy devono essere accessibili e comprensibili, e gli utenti devono essere informati su come i loro dati saranno utilizzati, con chi saranno condivisi e per quanto tempo saranno conservati. Le aziende devono anche garantire che i dati siano trattati in modo sicuro, adottando le migliori pratiche per la protezione dei dati e rispondendo prontamente a eventuali violazioni.

Un altro aspetto cruciale è la gestione delle preferenze degli utenti. Le aziende devono offrire strumenti che permettano agli utenti di gestire facilmente le proprie preferenze di consenso, adattandosi alle loro esigenze e desideri in modo flessibile e trasparente. Questo non solo rafforza la fiducia dei consumatori, ma contribuisce anche a una migliore esperienza utente.

Infine, la conformità alle normative sulla protezione dei dati deve essere vista non solo come un obbligo legale, ma come un'opportunità per differenziarsi nel mercato. Le aziende che dimostrano un impegno verso la privacy e la protezione dei dati possono ottenere un vantaggio competitivo, costruendo una reputazione di affidabilità e responsabilità. In un contesto in cui i consumatori sono sempre più attenti alla privacy, investire nella protezione dei dati è fondamentale per il successo a lungo termine.

In sintesi, un approccio etico e conforme alla normativa nella gestione dei dati personali non solo protegge i diritti degli individui, ma rappresenta anche un elemento distintivo di qualità e responsabilità per le aziende. La protezione dei dati personali deve essere integrata in ogni aspetto delle operazioni aziendali, promuovendo una cultura della privacy che valorizzi e rispetti i diritti dei consumatori. Solo così le aziende potranno navigare con successo nel complesso panorama della protezione dei dati, mantenendo la fiducia dei loro clienti e prosperando in un mercato sempre più competitivo e regolamentato.

Bibliografia

Bravo F., *Lo scambio di dati personali nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazioni e contratto*, Contratto e Impresa 2019.

Locoratolo B., *Il Trattamento Dei Dati Personali E La Privacy*, Simone, 2021.

Voigt, P., & Bussche, A. von dem. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

Warren, Samuel D., & Brandeis, Louis D., *The Right to Privacy*. Harvard Law Review, 1890

Wylie C., *Il Mercato Del Consenso*, Longanesi, 2019

Riferimenti normativi:

- Decreto Legislativo 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali";
- Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- Direttiva (UE) 2019/770 del Parlamento Europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali;
- 'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione - 24 febbraio 2005;
- Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- Linee Guida Cookie e altri strumenti di tracciamento, 10 giugno 2021, Gazzetta Ufficiale 163, 9 luglio 2021;
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e alla libera circolazione di tali dati (GDPR);
- Regolamento UE 2016 679. Arricchito con riferimenti ai Considerando Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018.

Sitografia

A. M. Lorito, M. Defidio, La comunicazione dei dati personali a terzi per finalità promozionali: gli ultimi provvedimenti del Garante tra conferme e novità, in "Dgrs.it, ultima modifica 2022, https://www.dgrs.it/la-comunicazione-dei-dati-personali-a-terzi-per-finalita-promozionali-gli-ultimi-provvedimenti-del-garante-tra-conferme-e-novita/

F. Corona, Diritto alla riservatezza: riconoscimento ed evoluzione normativa, in Legaldesk.it, ultima modifica 8/07/18 https://legaldesk.it/blog/diritto-riservatezza-evoluzione-normativa/

F. Pozzato, Cessione di dati personali per finalità di marketing, in "Dirittoprivacy.com", ultima modifica 2019, https://www.dgrs.it/la-comunicazione-dei-dati-personali-a-terzi-per-finalita-promozionali-gli-ultimi-provvedimenti-del-garante-tra-conferme-e-novita/

Saetta B., Consenso al trattamento, in "protezione dati personali, ultima modifica 10/10/23 https://protezionedatipersonali.it/consenso

Attilio Grilli A., Metodi e procedure in caso di acquisizione di aziende alla luce del GDPR, in "riskmanagement360", ultima modifica 12/10/2021, https://www.riskmanagement360.it/analisti-ed-esperti/metodi-e-procedure-in-caso-di-acquisizione-di-aziende-alla-luce-del-gdpr/

Bocchi C., Operazioni societarie e contratti di acquisizione: adempimenti privacy a carico degli attori interessati, in "cybersecurity360", ultima modifica 6/09/19, https://www.cybersecurity360.it/legal/privacy-dati-personali/operazioni-societarie-e-contratti-di-acquisizione-adempimenti-privacy-a-carico-degli-attori-interessati/

M. Mancosu, Cosa Sono I Cookie, in "ottimizzazione-pc.it", ultima modifica 2018, https://www.ottimizzazione-pc.it/cosa-sono-i-cookie/

A. Nucara, "Nuove Linee Guida sui Cookies: cosa cambia?", in "privacylab.it", ultima modifica 1/07/24, https://www.privacylab.it/IT/1247/nuove-linee-guida-sui-cookies-cosa-cambia/

M. Martorana, R. Savella, Cookie, nuove linee guida del Garante Privacy: 6 mesi per adeguarsi", in "Altalex.com", ultima modifica 20/07/21, https://www.altalex.com/documents/news/2021/07/20/cookie-nuove-linee-guida-garante-privacy-6-mesi-per-adeguarsi

Fusioni aziendali e GDPR: cosa fare in materia privacy, in "advisory360", ultima modifica 25/05/21, https://www.advisory360hub.it/blog/audit-compliance/dpo-as-a-service/fusioni-aziendali-e-gdpr-cosa-fare-in-materia-privacy/

Rossi, L., e Bianchi, M. (2019). *La protezione dei dati personali: Principi, regole e applicazioni pratiche del GDPR*. Milano: Franco Angeli.