Focus Team Alta Gamma

N.2 - aprile 2018

Focus Team Alta Gamma

Focus Team leader
Francesco Anglani
Francesco.Anglani@belex.com
Tel. 06-845511
02-771131

Autori
Giovanni Guglielmetti

Giovanni.Guglielmetti@belex.com
tel.: 02-771131

Fabia Cairoli
Fabia.Cairoli@belex.com
tel.: 02-771131

Milena Mursia
Milena.Mursia@belex.com
tel.: 02-771131

Carmine Trovato
Carmine.Trovato@belex.com
tel.: 02-771131

L'IMPATTO SULLE AZIENDE DEL LUSSO DEL REGOLAMENTO UE 679/2016 ("GDPR")

Ormai ci siamo: tra circa un mese (dal 25 maggio 2018) il GDPR diventerà applicabile in tutti gli Stati dell'Unione Europea.

Da un punto di vista generale, l'applicazione del GDPR pone vari problemi, primo tra tutti stabilire quali parti della vecchia disciplina nazionale e quali provvedimenti del Garante continueranno ad applicarsi anche dopo l'entrata in vigore della normativa europea.

Infatti, la disciplina nazionale dei singoli stati non uscirà completamente di scena: in alcune materie rimane ai singoli Stati un margine di intervento, ad esempio per l'individuazione dei casi in cui la valutazione di impatto è obbligatoria e per l'adozione di norme specifiche sul trattamento dei dati nel rapporto di lavoro. Inoltre, le autorizzazioni delle autorità nazionali di controllo rimangono in vigore finché non siano modificate, sostituite e abrogate.

Il 21 marzo 2018 il Consiglio dei Ministri ha approvato, in esame preliminare, uno schema di decreto legislativo che introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR. Il comunicato stampa del Governo conferma che il vigente Codice Privacy sarà abrogato, e al GDPR si affiancheranno le disposizioni attuative contenute nello schema di decreto. In ogni caso, anche le norme nazionali successive dovranno rispettare il GDPR, altrimenti dovrebbero essere disapplicate.

Inoltre, il Garante ha recentemente adottato Linee Guida sull'applicazione del GDPR per fornire agli operatori alcune raccomandazioni di carattere più operativo e pratico (ad es. indicazioni sui provvedimenti in materia di bilanciamento di interessi che continueranno ad applicarsi).

Nel poco tempo che ci separa dall'applicazione del GDPR, le imprese e gli altri operatori dovranno condurre un'attenta analisi dei processi interni e dei servizi offerti: nelle aree in cui la normativa privacy risulti modificata dal GDPR (informativa, base giuridica del trattamento, tempi di conservazione dei dati, misure di sicurezza, diritti degli interessati, etc.), sarà necessario **intraprendere le necessarie azioni di adeguamento**. La violazione della disciplina introdotta dal GDPR può comportare **sanzioni monetarie fino a 20 milioni di euro**

o al 4% del fatturato mondiale totale annuo, oltre a sospensioni e divieti dei trattamenti illeciti.

Come sono coinvolte le aziende del lusso?

Alcune delle novità introdotte hanno rilievo anche per le aziende di alta gamma, in quanto relative a trattamenti e strumenti anche delle aziende di tale settore. Tra queste citiamo la nomina del DPO, la profilazione, il registro dei trattamenti, il soft spam e le misure di sicurezza per il CRM.

1) Il Responsabile della Protezione dei Dati

Il Data Protection Officer ("**DPO**"), dovrà essere nominato quando l'attività principale dell'impresa consiste in trattamenti che per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio di persone, regolare, sistematico e su larga scala (ad es., profilazione e geolocalizzazione).

A prescindere dai casi in cui la nomina è obbligatoria, il DPO rappresenta un utile strumento per assicurare un presidio privacy e facilitare l'attuazione del GDPR, e la cui nomina è infatti incoraggiata anche dal Gruppo di lavoro "Articolo 29"[1]. Anche se il DPO viene nominato su base volontaria, dovrà comunque essere scelto nel rispetto dei criteri per la designazione, la posizione e i compiti previsti dal GDPR per i DPO designati in via obbligatoria.

- *Compiti del DPO*

I principali **compiti** del DPO, che dovranno essere indicati nell'atto di designazione, consistono nell'attività di indirizzo in merito agli obblighi derivanti dal GDPR, di sorveglianza e di interlocuzione con il Garante (art. 39 GDPR).

Parole chiave per il DPO:

(i) qualità professionali e

(ii) indipendenza

- *Chi può essere nominato DPO?*

Il DPO dovrà essere nominato dal titolare o dal responsabile del trattamento, e dovrà essere scelto per le sue **qualità professionali** (adeguata conoscenza della materia) e capacità di operare con un grado sufficiente di **indipendenza** all'interno dell'organizzazione aziendale. Il DPO non potrà essere scelto tra i soggetti che decidono sulle finalità e modalità del trattamento, non dovrà ricevere istruzioni sulle condotte da tenere - quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno il Garante - e dovrà essere in grado di riferire direttamente al vertice gerarchico del titolare o del responsabile del trattamento.

[1] Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017.

Il DPO potrà essere interno e alle dipendenze del titolare del trattamento, o esterno, e in quest'ultimo caso la designazione farà parte integrante di un apposito contratto di servizi. Il Garante suggerisce[2] che nel caso di DPO interno, ove la struttura organizzativa lo consenta e tenuto conto della complessità dei trattamenti, sia designato un dirigente di alta professionalità, che si rapporti direttamente con il vertice dell'organizzazione.

Meglio un DPO interno o esterno all'azienda?

Nella scelta tra DPO interno o esterno occorrerà tenere conto di diverse considerazioni. Anzitutto, il titolare dovrà designare il DPO evitando l'insorgere di situazioni di conflitti di interesse. Il Garante ritiene[3] sia preferibile evitare di assegnare il ruolo di DPO a funzioni manageriali di vertice all'interno dell'organizzazione (quali amministratore delegato, membro del consiglio di amministrazione, responsabile operativo, responsabile finanziario), o delle strutture che hanno potere decisionale in merito alle finalità o modalità del trattamento (ad esempio direzione marketing, direzione risorse umane, responsabile IT), mentre è da valutare, in base alle circostanze, l'assegnazione dell'incarico di DPO ai responsabili delle funzioni di staff, tra cui il responsabile della funzione legale. Anche nel caso in cui si opti per un DPO esterno occorre porre attenzione a evitare situazioni di conflitto di interesse, come nel caso in cui al DPO esterno si chiedesse di assistere il titolare in un giudizio che riguardi anche problematiche privacy[4].

Inoltre, la dimensione e la complessità della struttura organizzativa possono del pari incidere sulla scelta: da una parte un DPO esterno potrebbe essere dotato di maggiori risorse ed esperienze (lavorando su più fronti e quindi conoscendo anche altre realtà aziendali), dall'altra un DPO interno potrebbe avere una maggiore conoscenza dell'organizzazione e dei trattamenti, una più agevole accessibilità alle informazioni, oltre che una maggiore dimestichezza con le dinamiche interne che potrebbe consentire un più pronto intervento.

Ma c'è una terza via: un DPO esterno e figure interne di supporto

Per realizzare i vantaggi delle due opzioni si potrebbe scegliere di designare un DPO esterno, prevedendo adeguate garanzie di indipendenza nel contratto di servizi e, al contempo individuare una serie di figure interne all'azienda che operino come referenti per il DPO.

---

[2] Si vedano le Nuove Faq sul Responsabile della Protezione dei dati in ambito pubblico. Riteniamo che queste raccomandazioni, seppure fornite dal Garante per il settore pubblico, possano rappresentare un utile riferimento anche per il settore privato.

[3] Si vedano le Nuove Faq sul Responsabile della Protezione dei Dati in ambito privato, 26 marzo 2018.

[4] Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017.

In ogni caso, in ragione della complessità dei trattamenti, un ufficio formato da un team di lavoro potrà assistere il DPO nello svolgimento dei suoi compiti, ferma restando la necessità che venga sempre individuata una figura che assuma la funzione di DPO.

Una volta designato il DPO, i suoi dati di contatto dovranno essere forniti agli interessati (nelle informative e/o sul sito del titolare/responsabile del trattamento) e comunicati al Garante. Sarà poi buona prassi fornire agli interessati anche il nominativo del DPO[5].

2) Come descrivere le logiche di profilazione nelle informative ai clienti

Un'altra delle novità introdotte è l'obbligo per il titolare di fornire agli interessati informazioni di maggiore dettaglio sui trattamenti cui vengono sottoposti i suoi dati, tra cui informazioni sulla logica di profilazione utilizzata nel trattamento, nonché sull'importanza e le conseguenze previste per l'interessato. A tale proposito precisiamo che:

- **non è necessaria una spiegazione analitica** delle procedure utilizzate, ma le informazioni devono essere sufficientemente specifiche affinché il destinatario sia posto in grado di comprendere come i suoi dati vengono trattati. Per esempio, il titolare dovrà fornire l'indicazione:

  (i) delle caratteristiche principali considerate nel prendere una decisione, la fonte delle informazioni (ad es., in parte fornite dall'interessato e in parte raccolte da registri pubblici) e quanto tali informazioni rilevano nel processo di "valutazione";

  (ii) del fatto che il sistema usato viene testato periodicamente per assicurarne l'imparzialità e l'efficacia; e

  (iii) in caso di decisione che non soddisfa l'interessato, dei contatti cui lo stesso può rivolgersi per ottenere l'intervento umano, esprimere la propria opinione o contestare la decisione;

- il titolare è tenuto a illustrare come, a fronte di certi comportamenti, derivi una precisa conseguenza, anche fornendo esempi concreti (ad es., i prodotti appariranno all'interessato tenendo conto delle preferenze manifestate in precedenti esperienze di navigazione).

[5] Esiste un vero e proprio obbligo di comunicare il nominativo del DPO agli interessati in caso di violazioni dei dati personali (art. 33, par. 3, lett. b GDPR).

3) Come impostare un registro dei trattamenti per il marketing

L'art. 30 del GDPR impone di tenere un registro dei trattamenti, (l'obbligo non si applica alle imprese con meno di 250 dipendenti, a meno che le stesse effettuino un trattamento che può presentare un rischio per i diritti e le libertà degli interessati, non sia occasionale o includa dati sensibili). Le informazioni da inserire nel registro dei trattamenti corrispondono quasi del tutto a quelle che erano oggetto di notificazione al Garante per specifici trattamenti ai sensi dell'art. 37 del Codice della Privacy: considerando che la notificazione era obbligatoria per trattamenti come la profilazione e la geolocalizzazione e non per il marketing, è ragionevole pensare che quest'ultimo non sia da considerare un trattamento "a rischio". In ogni caso, tenendo conto da un lato che il Garante incoraggia la redazione di un registro dei trattamenti a prescindere dalle dimensioni dell'organizzazione[6], e che, dall'altro, la tenuta di un registro costituisce uno strumento per la mappatura dei trattamenti ed è quindi utile anche in chiave di accountability, appare raccomandabile provvedere alla tenuta del registro anche per i trattamenti per finalità di marketing.

Tra le informazioni da indicare nel registro dei trattamenti vi saranno le categorie di destinatari a cui i dati personali sono stati o saranno comunicati per svolgere l'attività di marketing (tra cui ad es. le società terze utilizzate per inviare le newsletter e il fornitore IT che conserva i dati) e i termini ultimi previsti per la cancellazione delle diverse categorie di dati (il Garante ha generalmente indicato per la conservazione dei dati per finalità di marketing 24 mesi, tuttavia in provvedimenti ad hoc ha acconsentito a termini più lunghi - ad es., nei casi di aziende che commercializzano prodotti o servizi di lusso, quali gioielli, oppure nel settore immobiliare, sono stati concessi tempi di conservazione fino a 10-15 anni).

Non sono prescritte forme particolari e vincolanti per il registro, qualsiasi forma idonea potrà essere adottata.

4) Il *soft spam* sopravvive al GDPR?

La proposta di Regolamento e-Privacy fa salva questa forma di trattamento[7]. Dunque, le imprese che nel contesto della vendita di un

[6] Tra l'altro, il considerando 82 del GDPR richiede genericamente al titolare di tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità.

[7] Il considerando 33 del Regolamento e-Privacy cita: "*However, it is reasonable to allow the use of e-mail contact details for electronic message within the context of an existing customer relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details for electronic message in accordance with Regulation (EU) 2016/679*". Si veda anche il considerando 47 del GDPR che considera il legittimo

Contatti del FT Alta Gamma

Francesco Anglani, FT leader
Francesco.Anglani@belex.com

Alessandro Balp
Alessandro.Balp@belex.com

Elena Busson
Elena.Busson@belex.com

Stefano Cacchi Pessani
Stefano.CacchiPessani@belex.com

Marcello Giustiniani
Marcello.Giustiniani@belex.com

Giovanni Guglielmetti
Giovanni.Guglielmetti@belex.com

Marco Maniscalco
Marco.Maniscalco@belex.com

Fulvio Marvulli
Fulvio.Marvulli@belex.com

Alessandra Piersimoni
Alessandra.Piersimoni@belex.com

Stefano Simontacchi
Stefano.Simontacchi@belex.com

Silvia Stabile
Silvia.Stabile@belex.com

prodotto o della fornitura di un servizio hanno ottenuto legittimamente l'indirizzo email di un cliente, potranno avvalersene per inviargli nuove comunicazioni come ad es. newsletter, senza richiedere preventivamente il consenso, a patto che rispettino i seguenti requisiti:

- i messaggi promozionali potranno essere inviati via email. È esplicitamente escluso l'utilizzo di altri mezzi quali il telefono o l'invio di sms, per la posta tradizionale attualmente consentita in Italia occorrerà attendere la posizione assunta dal Garante.

- i servizi o prodotti offerti dovranno essere analoghi a quelli precedentemente venduti. Qualora il cliente abbia acquistato un abito da sera ad esempio, sarà possibile proporre l'acquisto di una *pochette* o un servizio di *make-up*.

- il cliente, deve essere adeguatamente informato della possibilità di rifiutare il soft spam, e non deve aver manifestato la sua opposizione.

5) Come predisporre le misure di sicurezza per il *Customer Relationship Management* (CRM)

Con riferimento alle misure di sicurezza, è importante ricordare che non sarà più sufficiente adeguarsi agli standard del vecchio Allegato B del Codice della Privacy, ma l'operatore dovrà adottare "*misure adeguate a garantire un livello di sicurezza adeguato al rischio*". Sarà dunque l'operatore che dovrà dimostrare di aver adottato le tecniche più avanzate al fine di dimostrare che i dati siano sufficientemente protetti da eventuali minacce, anche tenuto conto dei costi.

Tra le misure che potranno essere adottate:

- la pseudonimizzazione e la cifratura dei dati;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di intrusione informatica;
- una procedura per verificare che le misure adottate siano sempre aggiornate;
- la strutturazione di database in modo da garantire un tempo di conservazione dei dati conforme alla normativa privacy (ad esempio 24 mesi per finalità di marketing e 12 per la profilazione, ma anche termini più lunghi se giustificabili in base alla particolare tipologia dei prodotti e alla periodicità degli acquisti).

---

interesse come possibile base giuridica del trattamento per finalità di marketing diretto.