Esiste l’informativa privacy perfetta?

Uno degli aspetti fondamentali del Regolamento Europeo per la Protezione dei Dati (Reg. UE 679/2016, noto anche come GDPR) è costituito da Diritti dell’interessato, i cui requisiti sono descritti al Capo III del Regolamento stesso. Ed uno dei principali documenti (forse il principale) che ogni organizzazione ha predisposto per dimostrare il corretto adempimento a questo elemento è costituito dall’**Informativa**.

In realtà il Regolamento, agli articoli 12, 13 e 14 non cita il termine “Informativa”, ma “informazioni da fornire all’interessato”, ma ciò non cambia la sostanza, per cui quasi tutte le organizzazioni del nostro Paese, forse anche per continuità con la normativa precedente (D. Lgs 196/2003), hanno predisposto una o più informative per il trattamento di dati personali.

Ma vediamo un po’ cosa si vede in giro nelle varie informative che riceviamo ormai tutti i giorni dai siti internet (normalmente chiamate privacy policy), da tutti quelli a cui, per un motivo o per l’altro, lasciamo i nostri dati anagrafici, dagli ambulatori medici dove facciamo visite ed esami e così via.

Purtroppo, il panorama è molto vasto e variegato e talvolta ci mostra quanto il soggetto a cui forniamo i nostri dati personali sa di privacy.

Partiamo dalle informative intitolate “Informativa al trattamento dei dati personali ai sensi dell’art. 13 del D.Lgs 196/2003 e del regolamento UE 679/2016”. Diffidate dai contenuti di tali informative perché probabilmente sono un collage primordiale dell’informativa della vecchia normativa e di quella nuova, infatti il D.Lgs 196/2003 è stato sì novellato dal D. Lgs 101/2018, per cui è rimasto in vigore, ma l’articolo 13 di suddetto decreto è stato abrogato proprio dal D. Lgs 101/2018, evidentemente perché in contrasto con il GDPR che, per una strana combinazione, all’articolò 13 riporta contenuti analoghi.

Passiamo ora a commentare come il testo del Regolamento viene applicato.

Articolo 13 – Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

I dati del titolare del trattamento sono riportati in praticamente tutte le informative, anche se purtroppo il GDPR non ci indica chiaramente cosa si intende con "dati di contatto". La normativa prevede che debba essere agevole rivolgersi all'interessato per esercitare i propri diritti e probabilmente il solo indirizzo di posta elettronica non permetterebbe a tutti di contattare il titolare del trattamento, meglio riportare anche un indirizzo fisico e un numero di telefono.

Alcune informative, poi, riportano erroneamente il nome e cognome di una persona fisica (titolare dell'azienda, legale rappresentante, amministratore delegato?) al posto della ragione sociale della società che ricopre il ruolo di titolare del trattamento.

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

Su questo punto se ne vedono delle belle: capita che il RPD o DPO sia identificato nella persona che fa le veci del titolare (o legale rappresentante dell'azienda, o amministratore delegato), cosa esplicitamente vietata dalle linee guida sulla figura del DPO (*Data Protection Officer*).

In realtà il GDPR chiede solo i dati di contatto del RPD, per cui molti indicano solo un indirizzo di posta elettronica (del tipo dpo@azienda.it) come dato di contatto del DPO, un po' poco per i motivi sopra illustrati relativamente al titolare del trattamento. Comunque, non è espressamente vietato omettere il nome del DPO o la ragione sociale della persona giuridica che ha assunto l'incarico come DPO esterno.

Si consideri che il DPO dovrebbe essere una figura indipendente da poter contattare anche in modo riservato, soprattutto se si tratta di personale dipendente. Dunque, dovrebbe essere messo a disposizione degli interessati un canale con adeguata riservatezza (e-mail dedicata che legge solo il DPO, telefono diretto, anche fornito solo su richiesta, ecc.).

Non sta scritto da nessuna parte che i dati di contatto del DPO debbano stare nell'Informativa, proprio per i motivi indicati inizialmente (si tratta di informazioni da fornire all'interessato), per cui una brillante soluzione potrebbe essere quella di indicare il nominativo ed i dati di contatto del DPO in apposita

sezione del sito internet (soprattutto per Pubbliche Amministrazioni). In tal modo si evita di ripeterlo in tutte le informative e, siccome il DPO teoricamente potrebbe cambiare, si evita di modificare tutte le informative allorquando l'incarico di RPD dovesse passare ad altro soggetto.

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

Su questo punto si ritrovano diverse versioni, alcune più di stampo giuridico, altre più di tipo organizzativo-gestionale.

Occorre anticipare che – per un determinato titolare del trattamento – la scelta di predisporre una o più informative dipende dalle categorie di soggetti interessati (clienti, fornitori, dipendenti,…) e dalle finalità di trattamento (al limite un'informativa per ogni finalità).

Le finalità del trattamento possono essere rese semplicemente indicando a quale scopo sono trattati i dati personali, quindi – ad esempio – "i dati sono trattati per adempiere ad obblighi contrattuali o precontrattuali" e "per adempiere ad obblighi contabili e fiscali", oppure – nel caso dei dati di dipendenti – "per la gestione del rapporto di lavoro e requisiti di legge ad esso correlati".

La base giuridica del trattamento fa riferimento ai motivi di liceità del trattamento, riportati all'art. *6 del GDPR:*

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

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, in particolare se l'interessato è un minore.

Purtroppo, si vedono alcune informative che riportano testualmente che "la base giuridica del trattamento è quella determinata dall'art. 6 paragrafo 1 f) del GDPR" o qualcosa di simile, riportando l'esatta dicitura dell'art. 6 comma 1 e lettera applicabile. Ma che ne è della trasparenza e della chiarezza ("intelligibile", "linguaggio semplice e chiaro") delle informazioni da rendere all'interessato?

Anche riportare nello specifico quelli che sono i requisiti di legge che impongono il trattamento pare un esercizio inutile, anche perché non sarebbe certo facile.

Purtroppo, molti autori di informative (responsabili privacy interni, consulenti privacy esterni, ecc.) tendono a far prevalere la loro formazione di tipo legale ed a voler riportare tutti i riferimenti di legge, ma personalmente credo che debba essere dato maggior risalto alla chiarezza dell'informativa, riportando finalità di facile comprensione per chiunque.

Attenzione a non omettere alcune finalità di trattamento non immediate, ma che potrebbero verificarsi nel recente futuro, come ad esempio le finalità di marketing per l'invio di newsletter informative sull'attività del titolare oppure la tutela del credito. Se non comprese nella prima informativa, tali finalità dovranno essere contemplate in una informativa successiva e ciò potrebbe non risultare efficace e nemmeno efficiente.

Chiaramente alcune finalità "accessorie" al rapporto commerciale con un cliente – nella fattispecie le finalità di marketing – normalmente hanno diverse basi giuridiche (legittimo interesse, consenso) per cui ciò va indicato nell'informativa, ma indicare il preciso riferimento dell'art. 6 del GDPR potrebbe da un lato non soddisfare il requisito di chiarezza di cui sopra, dall'altro potrebbe non essere sufficiente a dimostrare la validità della scelta. Probabilmente sarebbe opportuno, in caso di dubbio, giustificare la scelta della base giuridica su altro documento interno. In caso di legittimo interesse del titolare questa scelta di base giuridica va giustificata in un qualche documento interno relativo alla gestione della privacy, anche in relazione al bilanciamento fra questi ed il rispetto dei diritti dell'interessato.

Un aspetto poco chiaro di questi articoli del GDPR si può evincere dal paragrafo b) di cui sopra: "*il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso".* Ebbene, nel rapporto commerciale fra persone giuridiche (cliente-fornitore) il cliente tratta i dati delle persone fisiche che rappresentano i fornitori (nome, cognome, telefono aziendale, telefono cellulare, indirizzo e-mail,…) e, viceversa, il fornitore tratta dati analoghi delle persone che rappresentano il cliente (suoi dipendenti e collaboratori). In realtà entrambe dovrebbero rendere l'informativa sul trattamento di questi dati alle persone fisiche

che rappresentano il cliente/fornitore, ovvero gli interessati, ma essi “sono parte del contratto” o “dell’esecuzione di misure precontrattuali”, come die il Regolamento? Forse solo in modo indiretto, in quanto aventi un legame contrattuale con il cliente/fornitore. Questi dati personali, comunque, potrebbero ricadere nel successivo articolo 14 del GDPR, in quanto non vengono normalmente raccolti presso l’interessato, ma è l’azienda che li comunica alla controparte.

Occorre precisare, infine, che le condizioni di liceità sopra elencate non si applicano alle categorie particolari di dati (ovvero gli ex dati sensibili a cui si aggiungono i dati genetici e biometrici), per i quali ci sono altre basi giuridiche da considerare, ma le considerazioni da fare sono più o meno le stesse.

d) qualora il trattamento si basi sull’articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

Ancora, in caso di legittimo interesse come motivo di liceità del trattamento, vanno spiegati quali sono questi interessi legittimi. Tra essi vi sono le finalità di marketing diretto, ammesse dal GDPR, ma sotto determinate condizioni.

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

Qui l’informativa deve riportare l’indicazione di tutti i possibili soggetti a cui verranno comunicati i dati personali oggetto di trattamento. La scelta dovrebbe senz’altro ricadere sulle categorie di destinatari, perché salvo pochi casi di destinatari Pubbliche Amministrazioni (ad es. INPS e INAIL per i dati dei dipendenti) gli altri destinatari potrebbero cambiare nel corso del tempo (es. commercialista, consulente del lavoro, società fornitrice di servizi di assistenza informatica, ecc.).

Questo punto dell’informativa deve naturalmente essere coerente con l’analogo elemento del registro dei trattamenti ove sono riportati i destinatari o categorie di destinatari a cui i dati possono essere comunicati. È opportuno controllare sempre la corrispondenza di questi due elementi, soprattutto a fronte di modifiche del registro o dell’informativa.

Ricordiamo che alcuni dei destinatari dei dati personali saranno stati nominati Responsabili del trattamento ai sensi dell’art. 28 del GDPR, altri potranno essere Titolari autonomi, altri ancora semplici soggetti autorizzati al trattamento.

Sebbene in alcune informative siano riportate, fra i destinatari dei dati personali, i soggetti autorizzati interni all’organizzazione (dipendenti), a mio avviso questi non rientrano fra i destinatari che intende il GDPR: è ovvio che un’organizzazione faccia trattare i dati personali che raccoglie da personale interno a autorizzato a farlo e questo l’interessato lo sa. Lo scopo dell’informativa – in questo punto – è informare l’interessato a chi altri vengono comunicati/trasmessi i suoi dati

personali.

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

In questo punto c'è tutto o niente, ovvero: per molte realtà si informa semplicemente l'interessato che i suoi dati personali non verranno trasferiti presso organizzazioni internazionali e/o Paesi al di fuori dello Spazio Economico Europeo, per altre, invece, si apre il capitolo dei trasferimenti di dati fuori dalla UE con tutto quel che consegue, soprattutto dopo la sentenza Schrems II e le Raccomandazioni EDPB che sono seguite. Questo argomento esula dall'obiettivo di questo articolo e, tra l'altro è stato ampiamente trattato in altro articolo di questo sito.

Oltre a sottolineare il fatto che anche questo elemento è presente nel registro dei trattamenti, pertanto bisognerà verificarne la coerenza, vorrei soffermarmi su alcuni testi di informative che di fatto non dicono nulla.

Infatti, in alcune informative ho trovato frasi del tipo: "i suoi dati personali non saranno normalmente trasferiti fuori dallo SEE, ma qualora lo fossero saranno trasferiti solo in Paesi terzi per i quali esiste una decisione di adeguatezza della Commission Europea (ai sensi dell'art. 45 del GDPR), oppure se il trasferimento è soggetto a garanzie adeguate (ai sensi dell'art. 46 del GDPR)".

Non si dice molto e non si capisce se i dati sono effettivamente trasferiti fuori UE, dove e quali sono le garanzie adeguate (il GDPR e le successive Raccomandazioni EDPB le definiscono, ma l'interessato non deve essere un esperto della materia).

Oltre ai diffusissimi sistemi cloud ubicati fuori UE, sarebbe opportuno informare l'utente in caso di utilizzo di sistemi per l'invio di newsletter, piattaforme di collaborazione e videoconferenza, servizi di posta elettronica, ecc. che sfruttano datacenter in USA.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

Teoricamente queste informazioni dovrebbe ro essere fornite dopo aver raccolto i dati personali dell'interessato, ma praticamente nessuno le separa nell'informativa.

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i

criteri utilizzati per determinare tale periodo;

Qui alcune informative si limitano a riportare criteri estremamente vaghi, del tipo: "i dati vengono conservati per il tempo necessario previsto dalla legge". Non mi sembra sia questo lo spirito del Regolamento, ma questo è un argomento che dovrebbe essere trattato separatamente in quanto è molto difficile essere precisi nel fornire queste informazioni, soprattutto perché in un rapporto fra cliente e fornitore, ad esempio, i dati personali trattati sono di diversi tipi ed ognuno di essi potrebbe avere tempi di conservazione diversi. In questo punto (come in altri) il GDPR è troppo sintetico nel testo del requisito e sarebbe stata utile un'interpretazione ufficiale.

Anche questo elemento lo ritroviamo nel registro dei trattamenti, per cui attenzione alla congruenza fra i termini di conservazione (massimi).

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

L'interessato, proprietario dei dati personali oggetto dell'informativa, deve essere informato dei suoi diritti, magari non citando pedissequamente il testo del regolamento, ma spiegandogli, con parole semplici, che può accedere ai suoi dati personali, li può modificare, ne può chiedere la cancellazione, se non impedito dalla legge, ecc.

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

L'interessato deve essere informato che, se il trattamento è stato basato sul suo consenso, tale consenso può essere revocato in qualsiasi momento, senza effetti su quello che è avvenuto prima della revoca.

d) il diritto di proporre reclamo a un'autorità di controllo;

è necessario informare l'interessato che può proporre reclamo al Garante Privacy (ora GPDP) e quasi sempre viene indicato il sito internet dello stesso.

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

Come nella precedente normativa italiana (nella quale occorreva esplicitare se il

conferimento dei dati era obbligatorio), anche nel GDPR occorre specificare se l'interessato è obbligato a fornire i suoi dati personali, tutti quelli richiesti o parte di essi, a seconda delle finalità di trattamento.

Naturalmente alcuni dati sono necessari per concludere un contratto, senza i quali il committente non può dar seguito alla richiesta di prodotti o servizi e nemmeno può adempiere ad obblighi legali in materia fiscale.

Si potrebbe discutere a lungo su determinati servizi, gratuiti, che sono subordinati alla fornitura di dati personali per finalità di marketing, ma questo è un altro discorso.

f) 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.

In questo punto, se applicabile, il linguaggio dell'informativa dovrebbe essere reso chiaro per l'interessato, in quanto non tutti hanno ben compreso il concetto di "profilazione" e che, comunque, si tratta di una decisione "automatizzata", ovvero presa da un algoritmo implementato in un software per computer.

Inoltre, gran parte delle informative riportano un capitolo sulle modalità del trattamento, nel quale si enunciano i criteri adottati dal titolare per tutelare i dati personali trattati.

Altro elemento non esplicitamente richiesto dall'informativa è costituito dalla tipologia di dati personali raccolti, sebbene la presenza di dati articolari (art. 9) o dati giudiziari (art.10) implichi una diversa base giuridica del trattamento e spesso la necessità di ottenere un consenso.

L'elencazione dei tipi di dati trattati potrebbe essere legata alla obbligatorietà o meno del conferimento di ogni tipologia di dati (ad es. i dati anagrafici sono necessari, i recapiti cellulare o mail no).

Da ultimo restano due aspetti da considerare:

1. Quante informative predisporre per i vari trattamenti?
2. Come dare evidenza che l'informativa è stata resa all'interessato?

Partiamo da quest'ultimo punto: il Regolamento non richiede la sottoscrizione dell'informativa da parte dell'interessato (sarebbe quasi un consenso) che, pertanto può rifiutarsi di farlo. Allora si può dimostrare di aver reso l'informativa tramite l'invio via e-mail, la pubblicazione su sito internet o comunque dimostrando di avere una procedura che prevede che qualcuno fornisca l'informativa (necessariamente in forma scritta) all'interessato.

Purtroppo, in alcuni casi ci dicono “firmi questo per la privacy” e non ci chiedono nemmeno se ne vogliamo una copia!

In alcuni casi l’informativa può essere suddivisa in un’informativa breve, da fornire verbalmente, magari attraverso un messaggio registrato o in calce ad una e-mail, ed un’informativa completa, disponibile su sito web.

L’altro problema riguarda il proliferare delle informative per ogni trattamento o interessato oppure di cercare di raggrupparle per tipologia di interessati.

Teniamo presente che una buona parte delle informazioni contenute nelle informative vale per tutti i trattamenti o comunque per diversi soggetti di cui si trattano i dati. Di contro più informative si gestiscono, più si genera dell’entropia e si rischia di sbagliare e di essere inefficienti.

Vale un po’ il discorso fatto per il registro dei trattamenti: è opportuno accorpare i trattamenti omogenei in un unico trattamento (riga o record) del registro.

Se consideriamo un unico trattamento la gestione del personale dipendente con tutti i relativi adempimenti (gestione paghe, sicurezza sul lavoro, formazione, eventuale servizio mensa, polizze, ecc.) dall’assunzione alla cessazione del rapporto, analogamente faremo una stessa informativa che comprenda tutti i trattamenti di dati dei dipendenti, avendo cura di elencare tutte le categorie di destinatari a cui possono essere comunicati i dati personali per i vari ambiti. Quest’esempio, semplice e presente praticamente in ogni realtà aziendale, può essere esteso ad altri ambiti di trattamento.

Poi sarebbe utile rappresentare l’informativa in una forma grafica chiara e di facile interpretazione, magari con tabelle e simboli grafici che permettano all’interessato di sapere come vengono gestiti i propri dati personali per ognuna delle finalità riportate nell’informativa.