OSSERVATORIO
TMT·DATA PROTECTION
*di Morri Rossetti*

# Monthly Roundup

Luglio 2022

# MONTHLY ROUNDUP

## *Luglio 2022*

I principali aggiornamenti in materia di TMT & Data Protection del mese di Luglio 2022

---

## NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

- **EDPB e EDPS**

- European Health Data Space must ensure strong protection for electronic health data [Link]

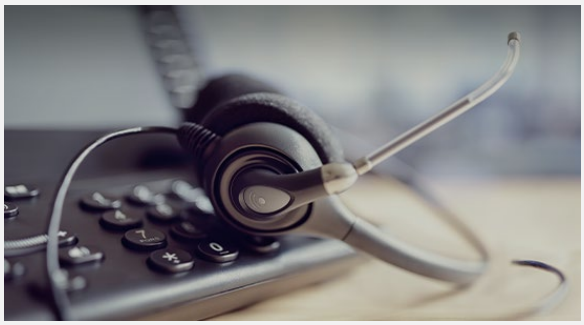
- **Garante Privacy**

- Tik Tok rinvia la pubblicità basata sul legittimo interesse. Per il Garante privacy "una decisione responsabile" - Comunicato del 12 luglio 2022

- Tik Tok: Altolà del Garante Privacy alla pubblicità "personalizzata" basata sul legittimo interesse. Base giuridica inadeguata e rischi che la pubblicità arrivi anche ai minori – Comunicato stampa dell'11 luglio 2022

---

## PRINCIPALI AGGIORNAMENTI



### Stop alle telefonate indesiderate: il registro delle opposizioni contro il telemarketing selvaggio sarà operativo da oggi

A partire da mercoledì 27 luglio, sarà operativo il nuovo registro pubblico delle opposizioni al *telemarketing* selvaggio ("**RPO**"), il quale semplifica le procedure per i cittadini che intendono tutelare la propria *privacy* da attività promozionali invasive e indesiderate.

Il nuovo RPO, estensione del servizio già messo a disposizione dei cittadini a partire dal 2010, è disciplinato dall'art. 4, comma 2, lett. a) del D.P.R. n. 26/2022, che ha attuato la L. n. 5/2018.

In particolare, l'ambito di applicazione del RPO – che include già il telefono fisso e l'indirizzo postale – verrà esteso anche ai numeri di telefono cellulare. In questo modo, in caso di iscrizione al registro, tutti i consensi all'utilizzo dei dati da

parte degli operatori verranno meno e questi ultimi saranno obbligati a consultare gli elenchi relativi ai consensi su base mensile e, in ogni caso, prima dell'avvio di ogni campagna pubblicitaria.

## Che cos'è il RPO?

Si tratta di un servizio pubblico e gratuito per tutti i cittadini che una volta iscritti negli elenchi del registro non potranno più essere contattati nemmeno al telefono cellulare dall'operatore di *telemarketing*, a meno che quest'ultimo non abbia ottenuto uno specifico consenso all'utilizzo dei dati successivamente alla data di iscrizione al RPO oppure nell'ambito di un contratto in essere o cessato da non più di trenta giorni, avente a oggetto la fornitura di beni o servizi, per il quale dovrà comunque essere assicurata, con procedura semplificata, la facoltà di revoca.

Tutte le imprese del settore iscritte al Registro degli Operatori di Comunicazione (il "ROC") [1] saranno tenute a verificare la lista del RPO e a eliminare dai loro database i contatti di coloro che non avranno prestato il consenso: le telefonate relative alle campagne pubblicitarie, quindi, potranno essere effettuate soltanto nei confronti dei numeri non presenti nel RPO.

In particolare, ai sensi della normativa applicabile, gli operatori che utilizzano i sistemi di pubblicità telefonica e di vendita telefonica o che compiono ricerche di mercato o comunicazioni commerciali telefoniche avranno l'obbligo di consultare il RPO mensilmente e, comunque, precedentemente all'inizio di ogni campagna promozionale, provvedendo, in seguito, all'aggiornamento delle proprie liste.

Saranno altresì vietati, con qualsiasi forma o mezzo, la comunicazione a terzi, il trasferimento e la diffusione di dati personali degli interessati iscritti al RPO, da parte dell'operatore di telemarketing, titolare del trattamento, per finalità pubblicitarie o di vendita ovvero per il compimento di ricerche di mercato o di comunicazione commerciale non riferibili alle attività, ai prodotti o ai servizi offerti dallo stesso.

In caso di violazione dei diritti dei soggetti registrati al RPO la normativa di riferimento prevede pesanti sanzioni. Infatti, in caso di abusi e violazioni, gli operatori di *telemarketing* rischieranno multe fino a 20 milioni di euro e, per le imprese, potranno essere irrogate sanzioni fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Sul punto si può ricordare che l'Autorità Garante per la protezione dei dati personali già nel 2020 aveva sanzionato una nota società italiana anche per aver effettuato, *inter alia*, telefonate promozionali senza consultare il RPO.

## Modalità di iscrizione al RPO

Dal punto di vista pratico, le chiamate degli operatori di *telemarketing* potranno essere bloccate dagli utenti tramite la richiesta di iscrizione, la quale potrà essere effettuata:

- gratuitamente;
- in qualsiasi momento (a partire da oggi);
- tramite la compilazione di un apposito modulo elettronico sul sito del RPO, oppure telefonando al numero verde 800 957 766 per le utenze fisse e allo 06 42986411 per i cellulari o inviando un apposito modulo digitale tramite mail

[1] Il ROC è un elenco istituito in Italia dalla L. n. 249, 1997, tenuto e regolamentato dall'Autorità per le Garanzie nelle Comunicazioni ("AGCOM"), al quale devono obbligatoriamente iscriversi i soggetti destinatari di concessioni o autorizzazioni in materia di comunicazione.

Tale registro ha la finalità di: (i) garantire la trasparenza e la pubblicità degli assetti proprietari; e (ii) consentire l'applicazione delle norme concernenti la disciplina anti-concentrazione, la tutela del pluralismo informativo e il rispetto dei limiti previsti per le partecipazioni di società estere.

all'indirizzo iscrizione@registrodelleopposizioni.it.

Ad ogni modo, restano comunque valide le iscrizioni inserite precedentemente al nuovo RPO, avendo l'utente anche la facoltà di annullare i consensi attraverso il rinnovo dell'iscrizione.

* * *

## AGCM: istruttoria nei confronti di Google per abuso di posizione dominante

Nell'adunanza dello scorso 5 luglio 2022, l'Autorità Garante della Concorrenza e del Mercato ("**AGCM**") ha avviato un'istruttoria nei confronti di Google (intesa quale complessivamente, Google LLC con sede in Irlanda, interamente posseduta e controllata da Alphabet Inc., società con sede nel Delaware (USA) e presente in Italia tramite la controllata Google Italy S.r.l., interamente posseduta da Google LLC) ipotizzando un abuso di posizione dominante e, pertanto, una violazione degli articoli 102 del Trattato sul Funzionamento dell'Unione europea ("**TFUE**") e 3 della legge 287/1990 (l'"Istruttoria").

Come è noto, Google è una società multinazionale che offre un'ampia gamma di prodotti e servizi connessi al mercato di Internet che comprendono tecnologie per la pubblicità online, strumenti di ricerca, *cloud computing*, software e hardware. Google detiene una posizione dominante in diversi mercati che consentono di acquisire grandi quantità di dati attraverso i servizi erogati (Gmail, Google Maps, Android) e nel 2021 ha realizzato un fatturato di 257,6 miliardi di dollari.

L'istruttoria è stata avviata a seguito di una segnalazione pervenuta all'AGCM da parte della società Hoda S.r.l. ("Hoda") società italiana, con sede a Milano, attiva nell'intermediazione di dati personali attraverso l'App denominata "Weople". In particolare, Weople è una App-banca dati che consente alle persone fisiche che si iscrivono a essa di immettere i propri dati in una sorta di conto e di beneficiare di un guadagno ogni volta che le imprese richiedono tali dati, in forma statistica, aggregata e anonima, per lo svolgimento della propria attività di targhettizzazione della clientela o per altri fini, come la creazione di database statistici o strumenti di *enrichment*.

L'attività di Hoda si basa, quindi, sulla raccolta e sulla disponibilità di un elevato numero di dati personali, sia forniti direttamente dagli utenti che creano il proprio account, sia raccolti dall'App attraverso l'interrogazione delle principali piattaforme internet o di erogatori di altri servizi e applicazioni digitali (sulla base di una delega conferita dall'utente a favore di Hoda). Come si legge nell'Istruttoria, tale meccanismo di interlocuzione tra l'App e i diversi operatori online avviene "*attraverso un protocollo tecnologico che consent[e] un dialogo e un aggiornamento continuo del flusso dei dati*".

In considerazione dell'importanza strategica acquisita dai dati, l'AGCM ha riconosciuto l'innovatività dei servizi offerti da Hoda – che consente agli utenti di valorizzare maggiormente i loro dati – affermando altresì la forza di mercato alternativa della stessa rispetto ai grandi aggregatori di dati online.

Nell'ambito dell'Istruttoria, l'AGCM ha individuato, pertanto, un'ipotesi di abuso di posizione dominante da parte di Google.

Nello specifico, Google avrebbe ostacolato l'interoperabilità nella condivisione dei dati presenti nella propria piattaforma con altre piattaforme, in particolare con l'App Weople, gestita da Hoda, la quale già dal 2019 aveva avviato contatti con Google "*per l'individuazione di meccanismi di interoperabilità in modo tale che l'utente Weople potesse indicare, anche con delega alla stessa Weople o direttamente dalla App, di trasferire i propri dati nel proprio account Weople, ai sensi dell'articolo 20, comma 2, del GDPR*".

Tuttavia, sebbene, come si legge nell'Istruttoria, sembrerebbe che Google stesse sviluppando un *framework* per garantire l'interoperabilità con altre piattaforme, è emerso che ad oggi l'unica modalità offerta da Google agli utenti per esercitare il loro diritto alla portabilità di dati fosse per il tramite di una procedura di Google raggiungibile solo direttamente e individualmente da ciascun utente attraverso un proprio account Google.

Tale unico meccanismo messo a disposizione da Google, per lo più considerato complesso e articolato, come segnalato da Hoda, avrebbe così avuto forti ripercussioni sul business della stessa.

## Articolo 20 del GDPR: Diritto alla portabilità dei dati

L'articolo 20 del Regolamento (UE) 2016/679 ("GDPR"), rubricato "*Diritto alla portabilità dei dati*", stabilisce che "*1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati. 2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. […]*"
Il diritto alla portabilità previsto dall'articolo 20 del GDPR è stato previsto dal legislatore europeo quale ulteriore strumento che consente all'interessato di rafforzare ulteriormente il controllo suoi propri dati personali qualora tali dati siano trattati con mezzi automatizzati, nei limiti di cui all'articolo 20 del GDPR (cfr. Considerando 68 del GDPR).
In ragione di ciò, viene fortemente incoraggiato lo sviluppo di formati interoperabili da parte dei diversi titolari del trattamento, sebbene non vi sia un obbligo specifico nei confronti degli stessi, che consentano la portabilità dei dati e che permettano all'interessato di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro.
Inoltre, come rilevato dall'AGCM, il diritto alla portabilità permette di facilitare la circolazione dei dati e la mobilità degli utenti, mitigando la grande disponibilità degli stessi a favore delle piattaforme più diffuse. Viene così riconosciuto anche il suo valore pro-concorrenziale nell'ambito dei mercati digitali: - - da un lato, offre a operatori alternativi di esercitare una pressione concorrenziale sugli operatori dominanti, quali Google;
- dall'altro, offre agli utenti la possibilità di conseguire il massimo potenziale economico conseguente all'utilizzo dei dati personali che, in particolare, può derivare da modalità economiche alternative di utilizzo degli stessi.

## Disponibilità dei dati e sfruttamento abusivo della posizione dominante di Google

L'articolo 102 del TFUE vieta lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una sua parte sostanziale, nella misura in cui ciò possa arrecare un pregiudizio al mercato intraeuropeo.

Nell'ambito dell'Istruttoria nei confronti di Google, l'AGCM ha dato avvio alla sua analisi partendo dalla considerazione che nel contesto dei mercati digitali, la principale leva concorrenziale è rappresentata proprio dalla disponibilità di un numero elevato di dati e dalla loro rilevanza e tali elementi sono altresì essenziali in quanto da essi dipendono caratteristiche fondamentali del servizio reso, in particolare in termini di innovazione e/o di personalizzazione. Tali valutazioni erano già state rilevate nell'ambito dell'indagine conoscitiva sui Big Data condotta congiuntamente dall'AGCM, dall'Autorità per le Garanzie nelle Comunicazioni e dal Garante per la protezione dei dati personali, conclusasi il 20 dicembre 2019.

Nel caso di specie, rileva come il ruolo svolto da Google nell'ecosistema digitale sia tale da garantirsi sempre un'ingente disponibilità di dati grazie alla vasta gamma di servizi offerti dalla stessa, idonea a soddisfare le diverse esigenze degli utenti e quindi in grado di falsare il gioco della concorrenza.

Infatti, sul punto, l'AGCM ha precisato che "*Mentre allo stato i dati acquisiti da Google vengono dallo stesso valorizzati nei mercati della pubblicità on-line, nei quali in particolare rappresentano l'elemento fondante della posizione dominante dell'operatore, in prospettiva l'applicazione in chiave pro-concorrenziale dell'istituto normativo della portabilità dei dati disciplinata dall'articolo 20 del GDPR apre agli utenti la possibilità di usufruire di diverse e ulteriori modalità di valorizzazione degli stessi. In particolare, in Italia l'attività di Hoda, ove non ostacolata da Google, potrebbe introdurre forme innovative di trattamento dei dati*".

Ne deriva che rispetto alla dominanza di Google sul mercato e, quindi, ai fini dell'applicazione dell'articolo 102 del TFUE (previa indagine condotta all'interno dell'Istruttoria sui mercati rilevanti), vi è posizione dominante quando sussiste una situazione di potere economico grazie alla quale l'impresa che la detiene è in grado di ostacolare il persistere di una concorrenza effettiva nei mercati rilevanti e di agire in maniera significativamente indipendente rispetto ai suoi concorrenti, ai suoi clienti e, in ultima analisi, ai consumatori.

## Le condotte in violazione dell'articolo 102 del TFUE

Alla luce degli elementi portati a conoscenza dell'Autorità e delle valutazioni condotte (come è noto, l'Istruttoria in esame non è il primo procedimento avviato – e conclusosi – nei confronti di Google), l'AGCM ha rilevato la possibile sussistenza di condotte poste in essere da Google in violazione dell'articolo 102 del TFUE.

"*Gli ostacoli frapposti da Google all'individuazione di meccanismi di interoperabilità idonei a rendere i dati presenti nella propria piattaforma disponibili a piattaforme alternative, nel pregiudicare l'esercizio, da parte dell'utente finale, del diritto alla portabilità dei propri dati, stabilito dal menzionato articolo 20 del GDPR, si risolve in un indebito sfruttamento, da parte della stessa Google, dei consumatori finali nella misura in cui determina una limitazione dei benefici che i consumatori potrebbero trarre dalla valorizzazione dei loro dati personali.*

*Tale condotta presenta un ulteriore carattere restrittivo della concorrenza nella misura in cui limita la possibilità di operatori alternativi a*

*Google di sviluppare forme innovative di utilizzo dei dati personali. In particolare, Hoda ha rappresentato i negativi effetti della condotta di Google sulla sua iniziativa volta a sviluppare, attraverso la piattaforma Weople, una innovativa attività commerciale, consistente nel valorizzare i dati personali con l'autorizzazione del suo titolare in prospettive merceologiche ancora inesplorate, con particolare riferimento al contesto geografico nazionale".*

In tal modo, Google preserverebbe la propria posizione nello sfruttamento commerciale dei dati resi a essa disponibile e ostacolerebbe lo sviluppo di modalità alternative di valorizzazione dei dati, e dunque l'esplicarsi di una concorrenza effettiva.

In particolare, l'AGCM ha rilevato come il complesso sistema di portabilità strutturato da Google non sembri rappresentare un valido sistema per garantire l'operatività dell'articolo 20 del GDPR. Infatti, nella misura in cui sussiste un valido consenso manifestato dall'utente ai sensi dell'articolo 20, paragrafo 2 del GDPR, Google, in quanto titolare del trattamento, è tenuta a porre in essere tutte le necessarie attività per garantire l'interoperabilità, essendo indifferente il profilo della modalità tecnica di realizzazione.

Tale mancanza fa così venire meno gli effetti pro concorrenziali della portabilità dei dati nell'ambito del settore digitale.

L'AGCM ha, quindi, concluso affermando che "*tale condotta, realizzata mediante la compressione del diritto, previsto dall'articolo 20 del GDPR, degli utenti alla portabilità dei propri dati personali, è suscettibile per un verso di pregiudicare in maniera considerevole le dinamiche concorrenziali in termini di livello dei servizi offerti, ampiezza e varietà dell'offerta, innovazione e diversità dei modelli di business, in tal modo ostacolando l'esplicarsi di una concorrenza basata sul merito, e per altro verso di sfruttare indebitamente i diritti dei consumatori, in violazione dell'articolo 102 del TFUE".*

## Conclusioni

L'attenzione prestata da parte delle diverse istituzioni e autorità, europee e nazionali, nei confronti delle grandi piattaforme digitali è ormai nota.

In particolare, la regolamentazione del mondo digitale avviata dall'Unione europea tramite l'introduzione di una serie di provvedimenti interconnessi, tra cui è possibile annoverare il Digital Market Act e il Digital Services Act è volta a garantire che gli utenti digitali abbiano accesso a prodotti e contenuti sicuri, nonché a proteggere i diritti fondamentali degli stessi; e ad assicurare il rispetto dei principi di libero mercato e della concorrenza nei settori digitali per stimolare l'innovazione e la crescita delle imprese all'interno del territorio europeo.

Nell'ambito del diritto della concorrenza, il Digital Market Act o DMA ha l'obiettivo di uniformare le opportunità di crescita delle imprese europee, indipendentemente dalla loro dimensione, tramite la regolamentazione delle società che controllano i punti chiave dei canali di distribuzione del mercato digitale e che hanno, pertanto, assunto una rilevanza notevole nel mercato (c.d. "*Gatekeeper*").

Le nuove norme stabiliscono degli obblighi e dei divieti che queste piattaforme dovranno rispettare nelle loro attività quotidiane. Tra i diversi obblighi previsti dalla DMA, i *Gatekeeper* dovranno rendere i propri servizi interoperabili per i terzi in situazioni specifiche.

***


## Comune sanzionato per trattamento illecito e mancata nomina del DPO

In data 12 maggio 2022, il Garante per la protezione dei dati personali (il "Garante" o l'"Autorità") ha emesso un'ordinanza ingiunzione nei confronti del Comune di Villabate (il "Comune"), sanzionandolo all'esito di un'istruttoria con cui ha accertato l'illiceità del trattamento dei dati personali di un ex dipendente e la mancanza di una valida designazione di un responsabile della protezione dei dati ("DPO"), in violazione degli artt. 5, par. 1, lett. a), 6 nonché gli artt. 37, parr. 1, lett. a), 7 e 38, par. 6, del Regolamento UE 679/2016 ("**GDPR**").

Con riferimento ai profili menzionati, trovano inoltre applicazione le "Linee Guida sul consenso ai sensi del Regolamento UE 2016/679", adottate dall'EDPB nel 2020, le "Linee Guida sui responsabili per la protezione dei dati", adottate dal Gruppo di lavoro Art. 29 nel 2016, nonché le "FAQ sul Responsabile della Protezione dei dati in ambito pubblico", adottate dal Garante.

### Descrizione del fatto

Il procedimento ha avuto origine dal reclamo presentato da parte di un ex dipendente del Comune (l'"Interessato"), attraverso il quale il medesimo aveva rappresentato che il Comune, nella persona dell'allora responsabile del settore Affari Generali, aveva inviato informazioni connesse al pignoramento del quinto del suo stipendio. Il responsabile del Comune, infatti, aveva comunicato tali informazioni al nuovo datore di lavoro dell'Interessato, e lo aveva informato dell'*"esistenza di presunti pignoramenti"*, *nonché dell'"esistenza di un residuo di presunto debito [...] scaduto e non trasmissibile fra le due amministrazioni*".

Il Comune aveva altresì contattato – per erronea convinzione che fosse un atto dovuto – l'istituto bancario creditore dell'Interessato informandolo non solo dell'avvenuta cessazione del rapporto di lavoro con l'Interessato stesso, ma anche di una serie di ulteriori informazioni di carattere personale a questo riferite, quali la proroga del periodo di aspettativa, la specifica ragione della cessazione del rapporto di lavoro per dimissioni volontarie e gli estremi del nuovo datore di lavoro.

Alla luce di quanto sopra e al fine di ricevere apposita tutela, l'Interessato si era pertanto rivolto al Garante, lamentando altresì che il Comune non aveva provveduto a designare un DPO o che, comunque, non aveva reso pubblici i dati di contatto, avendo l'Interessato stesso appreso solo in via informale che il soggetto individuato fosse la stessa responsabile del settore Affari Generali del Comune.

### Conclusioni del Garante

A seguito dell'attività istruttoria, il Garante ha rilevato quanto segue:

- con riguardo alla liceità del trattamento, il Comune, in qualità di titolare del trattamento, era tenuto, in ogni caso, a rispettare i principi in materia di protezione dei dati, fra i quali quello di liceità, correttezza e trasparenza, nonché di minimizzazione dei dati e tali dati personali dovevano pertanto essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato e dovevano essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali erano stati trattati. Il

Comune, tuttavia, avendo reso noto all'istituto bancario creditore informazioni di carattere personale riferite all'Interessato, aveva effettuato una comunicazione non necessaria né giustificata alla luce del quadro normativo che disciplina l'istituto del pignoramento presso terzi e gli obblighi del datore di lavoro – in qualità di terzo pignorato. Altresì illecita risultava la comunicazione effettuata dal Comune al nuovo datore di lavoro dell'Interessato in merito alla circostanza che l'Interessato avesse un debito nei confronti dell'istituto bancario creditore, nonché relativamente alle altre informazioni di dettaglio riguardanti il pignoramento di quota dello stipendio, il residuo della somma da pagare, la gestione del precedente rapporto di lavoro. La comunicazione dei dati personali dell'Interessato da parte del Comune all'istituto bancario e al nuovo datore di lavoro dell'Interessato stesso risultava pertanto in violazione degli artt. 5, par. 1, lett. a) e 6 del GDPR poiché effettuata in maniera non conforme al principio di liceità, correttezza e trasparenza e in assenza di un'idonea base giuridica. Il Comune aveva, infatti, ritenuto – erroneamente – che il trattamento fosse necessario per l'esecuzione di un contratto, ex art. 6, par. 1, lett. b) del GDPR. Tuttavia, ha ribadito il Garante, il trattamento è necessario per l'esecuzione di un contratto qualora vi sia un collegamento diretto e obiettivo tra il trattamento dei dati e la finalità dell'esecuzione del contratto con gli interessati (cfr. "Linee Guida sul consenso ai sensi del Regolamento UE 2016/679"). Nel caso di specie, invece, il rapporto contrattuale coinvolgeva unicamente l'interessato e l'istituto bancario e non (i) il Comune, che era il terzo presso il quale era stato effettuato il pignoramento; (ii) il nuovo datore di lavoro dell'Interessato, che era del tutto estraneo ai rapporti contrattuali in essere tra l'Interessato e il creditore.

- con riguardo all'assolvimento degli obblighi relativi al DPO, la designazione di tale figura è sempre dovuta da parte dei soggetti pubblici e il soggetto designato può svolgere altri compiti e funzioni, fermo restando che il titolare del trattamento deve assicurarsi che i compiti e funzioni assegnatigli non diano adito a un conflitto di interessi (ex art. 38, par. 6, del GDPR). Il titolare del trattamento deve altresì pubblicare i dati di contatto del DPO e comunicarli all'autorità di controllo. Il Garante, tuttavia, ha constatato che:
    - il Comune aveva designato informalmente come DPO il responsabile del settore Affari Generali;
    - la nomina era stata formalizzata con l'adozione di una determinazione sindacale, ma era stato ribadito il carattere di temporaneità della designazione poiché il Comune era in attesa di individuare una idonea figura esterna;
    - la comunicazione dei dati personali oggetto di reclamo era stata effettuata con nota sottoscritta dal responsabile del settore Affari Generali, il quale svolgendo altresì la funzione di DPO si trovava in una condizione di conflitto d'interessi rispetto al ruolo apicale svolto nell'ambito dell'organizzazione del Comune;
    - nel corso dell'istruttoria svolta dal Garante, il Comune aveva designato un DPO esterno;

- il Comune aveva comunicato tardivamente al Garante tale nuova nomina e non aveva pubblicato i dati di contatto della funzione non rendendo, pertanto, il DPO facilmente raggiungibile dagli interessati;
- il Comune aveva pertanto violato gli artt. 37, parr. 1, lett. a), e 7, nonché 38, par. 6, del GDPR.

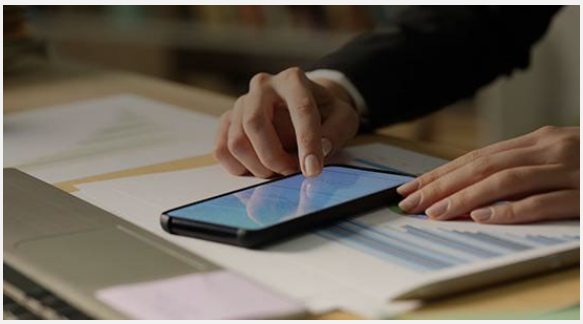
Le dichiarazioni in merito al trattamento, rese dal Comune nel corso dell'istruttoria, seppur meritevoli di considerazione, non sono state ritenute sufficienti per il superamento delle violazioni contestate riguardanti l'illiceità del trattamento di dati personali effettuato dal Comune, nonché per il mancato assolvimento degli obblighi relativi al DPO. Il Garante ha, infatti, evidenziato che il Comune (i) aveva comunicato a terzi i dati personali dell'Interessato in assenza di un'idonea base giuridica; (ii) non aveva tempestivamente adempiuto all'obbligo di designare un DPO; (iii) aveva nominato un DPO in posizione di conflitto d'interessi; (iv) aveva omesso di comunicare al Garante i dati di contatto del DPO; e (v) aveva omesso di pubblicare i dati di contatto del DPO sul proprio sito web istituzionale.

Con riferimento all'obbligo di designare un DPO nell'ambito pubblico, giova ricordare che l'Autorità, già in passato, aveva sanzionato la pubblica amministrazione – nello specifico il MiSE – per non aver, inter alia, designato il DPO entro il termine stabilito (vale a dire il maggio 2018, data di piena applicazione del GDPR) e per avere provveduto alla nomina e alla comunicazione al Garante dei dati di contatto con notevole ritardo[2].

### La sanzione amministrativa

Alla luce di quanto sopra, il Garante ha comminato una sanzione pari a Euro 6.000, ritenendo tale cifra effettiva, proporzionata e dissuasiva.

* * *



## Piattaforme di intermediazione e motori di ricerca: le Linee Guida dell'AGCOM e i nuovi poteri sanzionatori

Con la legge del 30 dicembre 2020 n. 178 (la "Legge di Bilancio 2021") che ha modificato l'art. 1, comma 6, lett. c) della legge del 31 luglio 1997 n. 249, introducendo il punto 14-bis, sono state affidate all'Autorità per le garanzie nelle comunicazioni (l'"Autorità" o "AGCOM") nuove competenze in materia di "*Platform to Business*" ("P2B")[3].

Nello specifico, all'AGCOM è stato affidato il compito di garantire l'adeguata ed efficace applicazione, da parte dei fornitori di servizi di intermediazione e dei fornitori di motori di ricerca online, del Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio dell'Unione Europea del 20 giugno 2019 (il "Regolamento P2B"), anche mediante l'adozione di linee guida,

2 Cfr. ordinanza di ingiunzione del Garante n. 54 dell'11 febbraio 2021, emessa nei confronti del Ministero dello Sviluppo Economico.

3 Con il termine P2B si individuano i rapporti in essere che si stabiliscono in caso di vendite online, tra i fornitori di servizi di intermediazione online e i motori di ricerca online e gli utenti commerciali, nonché i titolari di siti web aziendali che vendono i loro prodotti e servizi ai consumatori finali, utilizzando l'intermediazione delle piattaforme stesse.

la promozione di codici di condotta e la raccolta di informazioni pertinenti.

## Il Regolamento P2B

Il Regolamento P2B, che promuove l'equità e la trasparenza per gli utenti commerciali, è volto a tutelare gli utenti commerciali nonché i titolari di siti web aziendali che utilizzano i servizi di intermediazione online e i motori di ricerca online per lo svolgimento delle rispettive attività commerciali. L'obiettivo del legislatore europeo nell'emanazione del Regolamento è quello di garantire maggiore trasparenza nelle condizioni contrattuali applicate a coloro che fruiscono di tali servizi, anche in considerazione della dipendenza che i titolari di siti web aziendali hanno verso tali fornitori per poter offrire i propri beni e servizi a consumatori finali e utenti online.

In particolare, il Regolamento P2B individua nuovi obblighi in capo ai soggetti che forniscono tali servizi a coloro che hanno il luogo di stabilimento o di residenza nell'Unione europea e che, tramite tali piattaforme, offrono – a loro volta – beni o servizi ai consumatori del territorio dell'Unione europea (quali, a titolo esemplificativo e non esaustivo, specifiche misure a favore degli utenti commerciali per garantire trasparenza ed equità in merito ai termini e condizioni contrattuali applicabili, al posizionamento di beni e servizi offerti nel web e a eventuali trattamenti differenziati applicati ai prodotti o servizi offerti dai fornitori rispetto a quelli degli utenti commerciali, nonché efficaci mezzi per la risoluzione delle controversie che dovessero insorgere con gli utenti commerciali).

## Le Linee Guida dell'AGCOM

Nel recepire il compito affidatogli di garantire l'adeguata ed efficace applicazione del Regolamento P2B da parte dei fornitori di servizi di intermediazione online e dei fornitori di motori di ricerca online, l'AGCOM, con la Delibera n. 156/22/CONS del 19 maggio 2022, ha avviato la consultazione pubblica concernente le Linee Guida per l'adeguata ed efficace applicazione del Regolamento P2B (le "Linee Guida").

Le Linee Guida sono state predisposte con il fine di fornire indicazioni chiare circa le modalità di dettaglio per la predisposizione – da parte dei fornitori di servizi di intermediazione online – di termini e condizioni di fornitura dei servizi (i "T&C"), dei sistemi interni di gestione dei reclami e di mediazione, nonché per assicurare uniformità e coerenza nell'applicazione delle prescrizioni normative in vigore.

Nello specifico, i soggetti destinatari delle Linee Guida sono i seguenti:

- fornitori di servizi di intermediazione online, persone fisiche o giuridiche che, anche se non stabilite o residenti nel territorio nazionale, forniscono, od offrono di fornire, servizi di intermediazione online, come definiti dal Regolamento P2B, agli utenti commerciali stabiliti o residenti in Italia;
- motori di ricerca online che, anche se non stabiliti o residenti nel territorio nazionale, forniscono, od offrono di fornire, un servizio di ricerca online, come definito dal Regolamento P2B, in lingua italiana o agli utenti stabiliti o residenti in Italia.

Per la predisposizione dei T&C, i soggetti destinatari del Regolamento P2B saranno tenuti a consultare le Linee Guida e dovranno tenere in considerazione, inter alia, i seguenti profili:

- reperibilità, vale a dire che gli utenti (anche solo potenziali) dovranno poter reperire facilmente i T&C applicabili;
- comprensibilità, vale a dire che i fornitori dei servizi dovranno rendere disponibili agli utenti commerciali T&C redatti in un

linguaggio chiaro e leggibile, nonché in lingua italiana, se i servizi vengono forniti in Italia;

- completezza, con ciò intendendosi che i T&C dovranno consentire agli utenti commerciali di acquisire tutti gli elementi necessari ad assumere scelte informate e consapevoli, nonché ad ottenere un ragionevole grado di prevedibilità sugli aspetti più importanti della relazione contrattuale;
- modalità e tempistiche per le modifiche dei T&C, ovvero i fornitori di servizi dovranno comunicare le modifiche unilaterali delle condizioni contrattuali con un preavviso di almeno 15 giorni, salvo che le modifiche siano necessarie per adempiere a un obbligo normativo o per far fronte a un pericolo imminente connesso alla difesa dei servizi, dei consumatori e/o degli utenti commerciali da frodi, malware, spam, violazioni dei dati o rischi di sicurezza informatica e/o salvo l'estensione del periodo di preavviso in funzione della complessità e dell'impatto della modifica sull'attività o sulla fruizione del servizio da parte degli utenti;

limitazione, sospensione e cessazione della fornitura dei servizi, vale a dire che i T&C dovranno indicare espressamente le ragioni che giustificano la facoltà dei fornitori di sospendere, cessare o limitare, in tutto o in parte, la fornitura dei servizi della piattaforma online;

politiche di accesso ai dati adottate dai fornitori e, in dettaglio, le condizioni di accesso tecnico e contrattuale da parte degli utenti commerciali ai dati personali o a altri dati, o a entrambi, forniti dagli utenti commerciali o dai consumatori per l'uso dei servizi di intermediazione online in questione o generati tramite la fornitura di tali servizi. In particolare, i T&C dovranno chiarire espressamente, ad esempio, la possibilità o meno di (i) accesso ai dati personali e/o ad altri dati da parte dei fornitori di servizi di intermediazione online e/o degli utenti commerciali, (ii) accesso ai dati personali e/o ad altri dati anche in forma aggregata da parte degli utenti commerciali, (iii) condivisione con terzi di tali dati personali o degli altri dati raccolti;

informativa in merito al "posizionamento" dei beni o servizi offerti mediante i servizi di intermediazione online (c.d. ranking online), così come definito dal Regolamento P2B. A tal riguardo, l'AGCOM si è riservata di individuare ulteriori indirizzi in materia nell'ambito di un apposito tavolo tecnico, anche mediante l'adozione di codici di condotta;

istituzione di un sistema interno di gestione dei reclami degli utenti commerciali, da parte dei fornitori di servizi;

meccanismi di mediazione per il raggiungimento di accordi tra fornitori e utenti commerciali per la risoluzione di eventuali controversie nell'ambito della fornitura dei servizi.

In data 19 maggio 2022, è stato pubblicato il documento con il quale l'AGCOM ha avviato la consultazione pubblica della durata di 30 giorni. Tale consultazione è volta ad acquisire osservazioni ed elementi d'informazione, da parte dei soggetti destinatari, in merito alla proposta di provvedimento concernente le Linee Guida: esse potrebbero, infatti, avere un notevole impatto sulla loro operatività.

Allo stato attuale, l'AGCOM non ha ancora pubblicato un documento definitivo, successivo alla consultazione pubblica.

### I nuovi poteri sanzionatori

La Legge di Bilancio 2021 ha altresì stabilito che il presidio sanzionatorio, applicabile in caso di violazione di ordini o diffide impartiti dall'AGCOM in applicazione del Regolamento P2B, sia il medesimo previsto dalla legge del 31 luglio 1997 n. 249 per le violazioni in materia di posizioni dominanti.

Infine, la Legge di Bilancio 2021 all'art. 1, comma 517, ha esteso ai fornitori di servizi di intermediazione online e ai fornitori di motori di ricerca online che offrono servizi in Italia – anche se non stabiliti nel territorio nazionale – i seguenti obblighi e adempimenti:

obbligo d'iscrizione al Registro degli Operatori di Comunicazione ("ROC");
pagamento del contributo annuale all'Autorità;
comunicazione dell'Informativa Economica di sistema ("IES").

* * *

Per maggiori informazioni, potete contattare:

**Carlo Impalà**
*Partner e Responsabile Dip. TMT e Data Protection*
*(Carlo.Impala@MorriRossetti.it)*

OSSERVATORIO
TMT·DATA PROTECTION
*di Morri Rossetti*

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it