CRACA
DI CARLO
GUFFANTI
PISAPIA
TATOZZI
& ASSOCIATI

# PROFILI APPLICATIVI DELLA NUOVA NORMATIVA IN MATERIA DI *PRIVACY*

Corporate M&A 2017 Awards by legalcommunity
Best Practice Litigation

Finance 2017 Awards by legalcommunity
Studio dell'anno Finance Regulatory

Finance 2016 Awards by legalcommunity
Studio dell'anno Finance Regulatory

Corporate M&A 2016 Awards by legalcommunity
Studio dell'anno Litigation

## (1) Il nuovo quadro normativo

Dal 25 maggio 2018 diventa direttamente applicabile anche in Italia il Regolamento UE 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (il "**Nuovo Regolamento**"), relativo alla "*protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*".

Il Nuovo Regolamento è parte di un complessivo nuovo assetto normativo comunitario in materia di protezione di dati personali, che include anche la Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (la "**Nuova Direttiva**"), indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali.

Con la piena applicabilità il 25 maggio 2018 del Nuovo Regolamento sarà abrogata la Direttiva 95/46/CE, in attuazione della quale è stato emanato in Italia il testo normativo italiano di riferimento in materia, il D.lgs. 30 giugno 2003 n. 196 (il c.d. "**Codice Privacy**"). Da tale data ogni disposizione normativa nazionale, incluse le previsioni del Codice Privacy, incompatibile con il Nuovo Regolamento sarà abrogata e sostituita dallo stesso Nuovo Regolamento. Entro tale stessa data dovrà, inoltre, essere recepita dal legislatore italiano la Nuova Direttiva.

Il Nuovo Regolamento conferma i principi fondamentali alla base della precedente normativa e del Codice Privacy, introducendo, tuttavia, importanti novità e disposizioni di maggior dettaglio in molti ambiti.

In continuità con quanto già previsto dal Codice Privacy, le disposizioni del Nuovo Regolamento in materia di tutela degli "interessati" e "trattamento di dati personali" trovano applicazione soltanto nei confronti di persone fisiche (cfr. Considerando 14 e art. 1) ([1]).

([1]) Questa limitazione dell'ambito di applicazione del Codice Privacy è stata introdotta con il D.L. n. 201/2011 (convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214 - art. 40,

Via degli Omenoni, 2
20121 Milano
T +39 02 3041 331
F +39 02 3041 3333
www.5lex.it

Si riporta di seguito una sintesi di alcune delle principali novità introdotte con il Nuovo Regolamento che potrebbero avere impatti organizzativi per gli operatori e le società.

## (2) I nuovi compiti e responsabilità del Titolare e del Responsabile del Trattamento

Rispetto a quanto previsto dal Codice Privacy, il Nuovo Regolamento assegna al Titolare del Trattamento ([2]) un ruolo proattivo e obblighi più pregnanti, finalizzati all'adozione di tutti gli accorgimenti tecnici e organizzativi necessari a garantire la *compliance* effettiva dei trattamenti, anche sotto il profilo della sicurezza (c.d. principio di accountability). Al Titolare è affidato il compito di decidere autonomamente modalità e garanzie e limiti dei trattamenti dei dati personali, adottando e attuando misure tecniche e organizzative sin dal momento della progettazione, oltre che nell'esecuzione del trattamento (la c.d. "*data protection by default and by design*").

Inoltre, il Nuovo Regolamento introduce una disciplina più specifica e ampia riguardante il Responsabile del Trattamento ([3]), prevedendo, tra l'altro, alcuni obblighi specifici (ad es., l'adozione di idonee misure tecniche ed organizzative per garantire la sicurezza dei trattamenti), disciplinando più dettagliatamente le forme e modalità di nomina e consentendo anche la nomina di sub-responsabili del trattamento.

Infine, il Nuovo Regolamento disciplina la contitolarità del trattamento (art. 26 del Nuovo Regolamento), richiedendo anche ai Titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati.

## (3) Nomina di un Responsabile della protezione dati e Registro dei trattamenti

Il Nuovo Regolamento introduce in alcuni casi specifici un obbligo per il Titolare e il Responsabile del Trattamento di nominare un Responsabile della protezione dati (o *Data Protection Officer*). Il Responsabile della protezione dati ha compiti di supporto e sorveglianza per quanto riguarda le tematiche *privacy* e costituisce il "*punto di contatto*

---

comma 2). Prima di tale intervento normativo, infatti, le disposizioni in materia di trattamento dati personali del Codice Privacy si applicavano anche alle persone giuridiche.

([2]) Titolare del Trattamento è definito come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali" (art. 4(1), n. 7), del Nuovo Regolamento).

([3]) Responsabile del Trattamento è definito come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;" (art. 4(1), n. 8), del Nuovo Regolamento).

Via degli Omenoni, 2
20121 Milano
T +39 02 3041 331
F +39 02 3041 3333
www.5lex.it

*per l'autorità di controllo per questioni connesse al trattamento*" (art. 39, co. 1, lett. e), del Nuovo Regolamento). Esso dev'essere coinvolto in tutte le questioni riguardanti la protezione dei dati personali e riferisce direttamente al vertice gerarchico del Titolare o del Responsabile del Trattamento. L'obbligo di nomina del Responsabile è previsto quando (art. 37 del Nuovo Regolamento):

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del Titolare o del Responsabile del Trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del Titolare o del Responsabile del Trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati sensibili (di cui all'articolo 9) o di dati relativi a condanne penali e a reati (di cui all'articolo 10).

Il Nuovo Regolamento prevede, inoltre, in alcuni casi l'obbligo per i Titolari e i Responsabili del Trattamento di tenere uno specifico registro, contenente una serie di informazioni riguardanti i trattamenti svolti sotto la propria responsabilità (art. 30). Da tale obbligo di tenuta, tuttavia, sono esentate le imprese/organizzazioni con meno di 250 dipendenti, purché non effettuino "trattamenti a rischio" ([4]).

**(4) Contenuto e modalità di redazione dell'"informativa"**

Il Nuovo Regolamento ha introdotto nuove disposizioni in materia di "informativa", ossia del complesso di informazioni che il Titolare del Trattamento è tenuto a fornire ai soggetti di cui si appresta a trattare i dati.

In particolare, il Nuovo Regolamento ha previsto un'informativa di contenuto più ampio e dettagliato rispetto a quanto attualmente previsto dal Codice Privacy ed ha disciplinato in modo più dettagliato le modalità con le quali tale informativa deve essere redatta, richiedendo una forma concisa, trasparente, intellegibile per l'interessato e facilmente accessibile, e con linguaggio semplice e chiaro. Il Nuovo Regolamento ha, inoltre, disciplinato più precisamente le modalità di consegna di tale informativa agli

([4]) Ossia, "a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10" (art. 30(5) del Nuovo Regolamento).

Via degli Omenoni, 2
20121 Milano
T +39 02 3041 331
F +39 02 3041 3333
www.5lex.it

interessati, richiedendone in linea di principio la redazione per iscritto, anche in formato elettronico (art. 12 del Nuovo Regolamento), e consentendo espressamente che tali informazioni siano "*fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto*" ([5]).

**(5) Obblighi in caso di c.d. *data breach***

Il Nuovo Regolamento prevede un obbligo generalizzato (ossia, non più limitato ai "*fornitori di servizi di comunicazione elettronica accessibili al pubblico*") di comunicare l'avvenuta violazione di dati personali (c.d. *data breach*) al Garante per la protezione dei dati personali e, in determinati casi, anche al cliente (artt. 33 e 34 del Nuovo Regolamento).

L'obbligo di notifica al Garante deve avvenire senza ingiustificato ritardo, e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

**(6) Nuovi criteri di applicazione territoriale**

Il Nuovo Regolamento amplia significativamente l'ambito di applicazione territoriale della normativa comunitaria in materia di *privacy*. In particolare, si prevede l'applicazione del Nuovo Regolamento in caso di trattamento di dati personali di interessati situati in Unione Europea da parte di un Titolare o di un Responsabile del Trattamento non stabilito nell'Unione Europea, quando le attività di trattamento riguardano:

- l'offerta di beni/prestazione di servizi, anche a titolo gratuito, a soggetti nell'Unione Europea; oppure
- il monitoraggio del comportamento di soggetti nell'Unione Europea, ove il comportamento monitorato abbia luogo all'interno dell'Unione Europea.

Pertanto, alla luce della nuova disciplina vengono inclusi nell'ambito della normativa comunitaria anche operatori che, pur non svolgendo alcuna attività di trattamento di dati personali, né utilizzando comunque strumenti per tale trattamento all'interno dell'Unione Europea, indirizzano i propri servizi/beni nei confronti di persone fisiche situate in Unione Europea. Nell'ambito dell'offerta transfrontaliera di servizi e attività di investimento, o bancari, o assicurativi, la normativa in argomento troverà applicazione anche a quei soggetti che operino in libera prestazione di servizi.

([5]) Art. 12(7) del Nuovo Regolamento.

Via degli Omenoni, 2
20121 Milano
T +39 02 3041 331
F +39 02 3041 3333
www.5lex.it

Il Nuovo Regolamento, poi, si applica anche in caso di trattamento effettuato da uno "stabilimento" situato nell'Unione Europea (ad es., una *branch* o una società controllata) di un Titolare o Responsabile del Trattamento, anche se il trattamento è effettuato fuori dall'Unione Europea.

## (7) Prossimi adempimenti

Nei prossimi mesi si prevede l'emanazione di disposizioni normative di esecuzione da parte del legislatore comunitario e la pubblicazione di linee guide operative da parte di competenti organismi comunitari, tra cui il neo-costituito Comitato Europeo per la Protezione dei Dati (che sostituisce l'organo consultivo denominato «Articolo 29»), e del Garante italiano per la protezione dei dati personali. Inoltre, lo stesso Nuovo Regolamento incoraggia l'adozione da parte degli operatori di codici di condotta emanati da associazioni o organismi di categoria e l'acquisizione di certificazioni rilasciate da organismi di certificazione accreditati.

Ciascun operatore e società, quindi, è chiamata ad adeguarsi alla nuova normativa entro la data del 25 maggio 2018, adottando misure tecniche e organizzative e sistemi di sicurezza dei dati personali adeguati al proprio ambito di attività e profilo di rischio. In tale sforzo di adeguamento, sarà opportuno tener conto delle linee guida e indicazioni operative già emanate, e quelle che saranno emanate prossimamente, dai competenti organismi comunitari, dal Garante italiano e dalle competenti associazioni di categoria.

* * *

Via degli Omenoni, 2
20121 Milano
T +39 02 3041 331
F +39 02 3041 3333
www.5lex.it