

Nuovo Regolamento Ue sulla privacy. Dal Garante la prima Guida applicativa.

Sommario: I. Premessa; II. Fondamenti di liceità del trattamento; III.



Informativa; 3.1. Contenuto dell'informativa; 3.2. Tempi dell'informativa; 3.3. Modalità dell'informativa; IV. Diritti degli interessati; 4.1 Modalità per l'esercizio dei diritti (artt. 11 e 12); 4.2 Diritto di accesso (art. 15); 4.3 Diritto di cancellazione (diritto all'oblio) (art. 17); 4.4 Diritto di limitazione di trattamento (art. 18); 4.5 Diritto alla portabilità dei dati (art. 20); V. Titolare, Responsabile, incaricato del trattamento; VI. Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili; VII. Trasferimenti di dati verso paesi terzi e organismi internazionali.

Premessa

Il 25 maggio 2018 diventerà operativo il regolamento¹ Ue sulla privacy, approvato dall'Unione lo scorso anno. Si tratta di un regolamento che introduce nuove disposizioni immediatamente applicabili da tutti i Paesi, senza bisogno di passare per la procedura di recepimento, come invece è stato per le normative nazionali tuttora in vigore (in Italia si è iniziato con la legge 675 del 1996, che discendeva da una direttiva comunitaria, e poi si è passati al "Codice" del 2003 tramite il Dlgs. n.196 del 30 giugno 2003).

Il nuovo impianto del sistema europeo della privacy si comporrà di due parti: il regolamento (che riguarderà le persone fisiche, le imprese e le amministrazioni) e una direttiva² più mirata, relativa all'utilizzo dei dati personali nell'ambito della sicurezza, dell'attività di giustizia. Quest'ultima per essere tradotta in pratica, avrà, a differenza del regolamento, bisogno di essere recepita dai singoli Paesi³.

Per orientarsi nelle nuove regole europee il Garante della Privacy ha fornito una guida⁴ suddivisa in sei aree tematiche:

1. fondamenti di liceità del trattamento;
2. informativa;
3. diritti degli interessati;
4. titolare, responsabile e incaricato del trattamento;
5. *accountability*; e
6. trasferimento internazionale dei dati.

Fondamenti di liceità del trattamento

Il regolamento in esame conferma che ogni trattamento deve trovare fondamento in un'adeguata base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice (consenso, adempimento obblighi contrattuali, interessi

vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Non passano però inosservate alcune novità riguardanti il consenso:

- per i dati “sensibili”⁵ il consenso *dovrà* essere “esplicito”, lo stesso sarà anche per il consenso a decisioni basate su trattamenti automatizzati⁶;
- il consenso *non dovrà* essere necessariamente “documentato per iscritto”, né sarà richiesta la “forma scritta”, ma il titolare *deve* essere in grado di dimostrare che l’interessato ha prestato il consenso a uno specifico trattamento;
- il consenso dei minori è valido *a partire dai 16 anni*, prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Resta invariato che il consenso *debba* essere in tutti i casi, libero, specifico, informato e inequivocabile e *non è* ammesso il consenso tacito o presunto; inoltre, *dovrà* essere manifestato attraverso “dichiarazione o azione positiva inequivocabile”⁷.

Ebbene, il consenso raccolto precedentemente al 25 maggio 2018 resta valido qualora abbia tutte le caratteristiche sopra elencate; in caso contrario, sarà opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescritto dal regolamento⁸.

Informativa

Contenuti dell’informativa

I contenuti dell’informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento e sono stati in parte ampliati rispetto al vigente Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO¹⁰, inoltre, qualora sussista, la base giuridica del trattamento, qual è il suo interesse legittimo e se quest’ultimo costituisce la base giuridica del trattamento, nonché se si ha intenzione di trasferire i dati personali in Paesi terzi, ed in caso affermativo, attraverso quali strumenti.

Il Regolamento prevede anche ulteriori informazioni in quanto “necessarie per garantire un trattamento corretto e trasparente”: in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all’autorità di controllo. Qualora il trattamento comporti processi decisionali automatizzati (anche la profilazione), l’informativa dovrà specificarlo, indicando la logica di tali processi decisionali e le conseguenze previste per l’interessato.

Tempi dell’informativa

In caso di dati personali non raccolti direttamente presso l’interessato (art.14 del Regolamento), l’informativa dovrà essere fornita entro un termine ragionevole

(non oltre un mese dalla raccolta, o dal momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato))¹¹.

Modalità dell'informativa

Il Regolamento, rispetto al Codice, si sofferma maggiormente circa le caratteristiche dell'informativa, infatti prevede che la stessa informativa debba avere una forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; inoltre, specifica che occorre utilizzare un linguaggio chiaro e semplice, e che per i minori devono essere previste informative idonee (si veda considerando 58).

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, anche se sono ammessi anche "altri mezzi", pertanto, può essere fornita oralmente, ma sempre nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa in forma estesa (art. 12, paragrafo 7)¹². Sono inoltre parzialmente diversi anche i requisiti che il Regolamento fissa riguardo all'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1), anche se occorre sottolineare che spetterà al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato.

Diritti degli interessati

Modalità per l'esercizio dei diritti (artt. 11 e 12)

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile a 3 in caso di particolare complessità; il titolare dovrà comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Spetterà, quindi, al titolare di valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma solo nel caso di richieste manifestamente infondate, eccessive o ripetitive (art. 12.5), ovvero se sono richieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3).

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

Infine si ricorda che la risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre ad utilizzare un linguaggio semplice e chiaro.

Resta invariato il dovere di agevolare l'esercizio dei diritti in capo al titolare del trattamento nei confronti dell'interessato adottando ogni misura (tecnica e organizzativa) a ciò idonea.

Sono ammesse deroghe ai diritti riconosciuti dal Regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).

Diritto di accesso (art. 15)

Il diritto di accesso prevede il diritto di ricevere una copia dei dati personali oggetto di trattamento, fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorrerà indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

Diritto di cancellazione (diritto all'oblio) (art. 17)

Il cosiddetto "diritto all'oblio" si configura come un diritto alla cancellazione in forma rafforzata, è previsto l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, tramite la pubblicazione su un sito web), oltre alla cancellazione degli stessi, di informare della richiesta di cancellazione gli altri titolari che trattano i dati personali cancellati (si veda art. 17, paragrafo 2).

Diritto di limitazione di trattamento (art. 18)

Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

Diritto alla portabilità dei dati (art. 20)

È uno dei nuovi diritti introdotti dal Regolamento, tale diritto non si applica ai trattamenti automatizzati (quindi non si applica ad archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato o sulla base di un contratto stipulato con l'interessato, e solo i dati che siano stati "forniti" dall'interessato al titolare¹⁴. Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Titolare, responsabile, incaricato del trattamento

L'art. 26 del Regolamento disciplina la contitolarità del trattamento imponendo ai titolari di definire specificatamente¹⁶ le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento.

Il nuovo disposto normativo, infatti, fissa con maggior dettaglio (rispetto al precedente art. 29 del Codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: dovrà trattarsi, infatti, di un contratto (o di altro atto giuridico conforme al diritto nazionale) e dovrà disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti", quali, in particolare, la natura, durata e finalità del trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento.

Inoltre, è consentita la nomina di sub-responsabili del trattamento da parte di un

responsabile¹⁷, per specifiche attività di trattamento, sempre nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo, infatti, risponderà dinanzi al titolare dell'inadempimento del sub-responsabile¹⁸.

Sono previsti specifici obblighi in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un RPD-DPO, nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del Regolamento¹⁹.

Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili

Uno dei vari aspetti su cui si concentra il Regolamento è sicuramente la “responsabilizzazione” di titolari e responsabili circa l'adozione di comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione dello stesso²¹. Si tratta di una grande novità che riguarda la protezione dei dati, poiché viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, tutto ciò sempre rispettando le disposizioni normative nazionali nonché i criteri indicati nel Regolamento.

Fra tali attività risultano fondamentali quelle connesse al rischio inerente al trattamento, quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati²²; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale. L'autorità di controllo non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia. Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale

Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato sarà chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati²³.

Alcune delle principali novità, in termini di adempimenti da parte di titolari e responsabili del trattamento, saranno:

- a) la tenuta obbligatoria di un *Registro delle attività di trattamento* (art. 30 del Regolamento), fatta eccezione per le imprese o le organizzazioni con meno di 250 dipendenti che non effettuano trattamenti a rischio (art. 30, paragrafo 5). Il registro deve avere forma scritta (anche elettronica) e deve essere esibito su richiesta del Garante;
- b) dovranno essere garantite *misure di sicurezza* tali da garantire un livello di sicurezza adeguato al rischio del trattamento (art. 32);
- c) a partire dal 25 maggio 2018, tutti i titolari²⁴ dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo". Va ricordato che la notifica all'autorità non è obbligatoria ma è subordinata alla valutazione del rischio per gli interessati che spetta al titolare (si veda considerando 85);
- d) la designazione di un "*responsabile della protezione dati*" (RPD)²⁵.

Trasferimenti di dati verso paesi terzi e organismi internazionali

L'art. 45, paragrafo 1, del Regolamento prevede che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha valutato adeguato il livello di protezione garantito, in tal caso il trasferimento non necessiterà di alcuna autorizzazione specifica.

Venendo quindi meno il *requisito dell'autorizzazione nazionale*, la decisione della Commissione riguardo il trasferimento di dati verso un Paese terzo "adeguato" potrà avere inizio senza attendere l'autorizzazione nazionale del Garante²⁷. Tuttavia, tale autorizzazione sarà ancora necessaria se un titolare desidera utilizzare clausole contrattuali ad-hoc (quindi non riconosciute come adeguate tramite decisione della Commissione europea) oppure in caso di accordi amministrativi stipulati tra autorità pubbliche.

Il Regolamento consente di ricorrere anche a *codici di condotta ovvero a schemi di certificazione* per dimostrare le "garanzie adeguate" previste dall'art. 46. Ciò significa che i titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. Tuttavia, tali titolari dovranno assumere, inoltre, un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento che sia giuridicamente vincolante e azionabile dagli interessati²⁸.

La nuova normativa vieta espressamente il trasferimento di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze

amministrative emesse da autorità di tale Paese terzo, salvo l'esistenza di accordi internazionali²⁹, sarà sempre possibile ricorrere alle deroghe previste dall'art. 49, come nel caso di *interesse pubblico riconosciuto dal diritto dello stato membro del titolare* o da diritto dell'UE (art. 49, paragrafo 4).

Vengono fissati anche *i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme*. Va chiarito che l'elenco indicato a tal riguardo al paragrafo 2 dell'art. 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. L'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza previsto dagli artt. 63-65 del Regolamento.

Resta invece invariato l'approccio attualmente vigente in base alla direttiva 95/46/CE e al Codice italiano circa i flussi di dati al di fuori dell'Unione Europea e dello spazio economico europeo, prevedendo che tali flussi siano vietati, in linea di principio, a meno che intervengano specifiche garanzie che il Regolamento elenca in ordine gerarchico:

1. adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea (art. 44, comma 1, lettera b), del Codice);
2. in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello) (art. 44, comma 1, lettera a) del Codice);
3. in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (in parte corrispondenti alle disposizioni dell'art. 43, comma 1, del Codice).

Note:

¹ *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).

² *Direttiva* (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

³ Il Sole 24 Ore, *Sul nuovo regolamento europeo una guida del Garante della privacy*, di Antonello Cherchi, estratto da <http://www.ilsole24ore.com/art/notizie/2017-04-28/sul-nuovo-regolamento-europeo-guida-garante-privacy-120336.shtml?uuid=AEG5bDDB&fromSearch>, in data 30 maggio 2017.

⁴ Garante della Privacy, *Guida all'applicazione del regolamento europeo in materia di protezione di dati personali*, estratto da <http://www.garanteprivacy.it/guida-all->

[applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali](#), in data 30 maggio 2017.

Si veda l'art. 9 del Regolamento.

Deve essere ricompresa anche la profilazione, in tal senso si veda art. 22 del Regolamento.

⁷ Si vedano considerando 39 e 42 del Regolamento.

⁸ Garante della Privacy, *Fondamenti di liceità del trattamento*, estratto da <http://www.garanteprivacy.it/fondamenti-di-liceita-del-trattamento>, in data 30 maggio 2017.

⁹ Garante della Privacy, *Informativa*, estratto da <http://www.garanteprivacy.it/informativa>, in data 31 maggio 2017.

¹⁰ Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO).

¹¹ Diversamente da quanto attualmente previsto dall'art. 13, comma 4, del Codice vigente.

¹² Tali icone dovranno essere identiche per tutti i paesi dell'Unione e saranno definite prossimamente dalla Commissione europea.

¹³ Garante della Privacy, *Diritti degli interessati*, estratto <http://www.garanteprivacy.it/diritti-degli-interessati>, in data 31 maggio 2017.

¹⁴ Si veda il considerando 68 del Regolamento per maggiori dettagli.

¹⁵ Garante della Privacy, *Titolare, responsabile, incaricato del trattamento*, estratto <http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento>, in data 31 maggio 2017.

¹⁶ Attraverso un atto giuridicamente valido ai sensi del diritto nazionale.

¹⁷ Si veda art. 28, paragrafo 4.

¹⁸ Il responsabile primario risponderà anche ai fini di risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (art. 82, paragrafo 1 e paragrafo 3).

¹⁹ diversamente da quanto previsto oggi l'art. 5, comma 2, del Codice.

²⁰ Garante della Privacy, *Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili*, estratto <http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili>, in data 31 maggio 2017.

²¹ Si vedano artt. 23-25, in particolare, l'intero Capo IV del Regolamento.

²² Si vedano considerando 75-77.

²³ Si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati recentemente pubblicate dal Gruppo "Articolo 29", scaricabili al seguente [link:http://ec.europa.eu/newsroom/document.cfm?doc_id=44137](http://ec.europa.eu/newsroom/document.cfm?doc_id=44137).

²⁴ Non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi.

²⁵ Si veda art. 39 del Regolamento.

²⁶ Garante della Privacy, *Trasferimento di dati verso paesi terzi e organismi internazionali*, estratto <http://www.garanteprivacy.it/trasferimenti-di-dati-verso-paesi-terzi-e-organismi-internazionali> in data 31 maggio 2017. ²⁷ Come previsto dall'art. 44 dell'attuale Codice Privacy.

²⁸ Si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2.

²⁹ Si veda art. 48.

Milano, 10.07.2017

Avv. Cristina Biglia
Dott. Eugenio Mariani