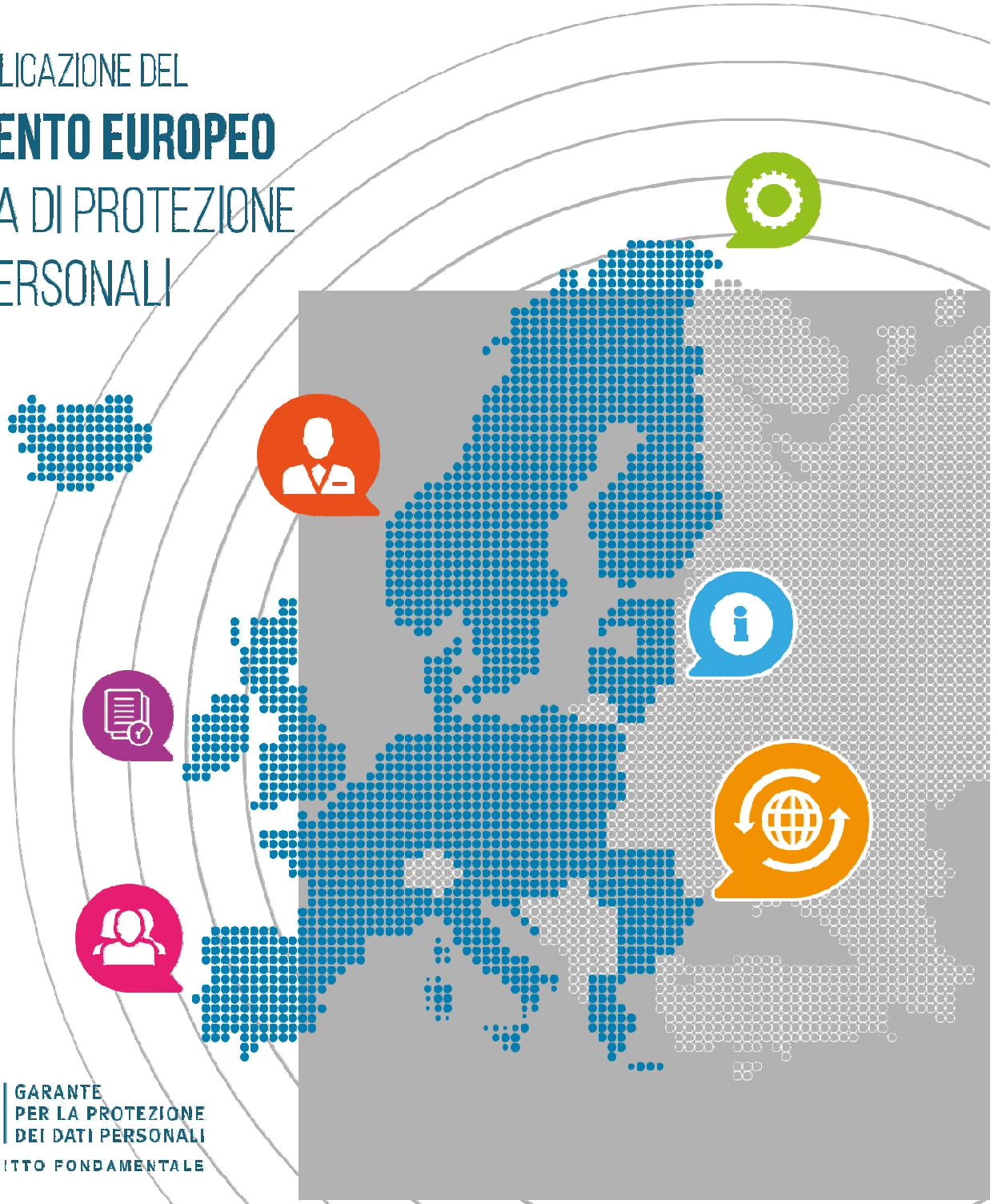
GUIDA ALL'APPLICAZIONE DEL

REGOLAMENTO EUROPEO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI



1997 2017

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Indice

Fondamenti di liceità del trattamento 4

Informativa 8

Diritti degli interessati 12

Titolare, responsabile, incaricato del trattamento 20

Approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili 24

Trasferimenti di dati verso Paesi terzi e organismi internazionali 30

Introduzione

La Guida intende offrire un panorama delle principali problematiche che imprese e soggetti pubblici dovranno tenere presenti in vista della piena applicazione del regolamento, prevista il 25 maggio 2018.

Attraverso raccomandazioni specifiche vengono suggerite alcune azioni che possono essere intraprese sin d'ora perché fondate su disposizioni precise del regolamento che non lasciano spazi a interventi del legislatore nazionale (come invece avviene per altre norme del regolamento, in particolare quelle che disciplinano i trattamenti per finalità di interesse pubblico ovvero in ottemperanza a obblighi di legge).

Vengono, inoltre, segnalate alcune delle principali novità introdotte dal regolamento rispetto alle quali sono suggeriti possibili approcci in modo da arrivare all'appuntamento del 25 maggio 2018 con le idee più chiare.

La presente Guida è soggetta a integrazioni e modifiche alla luce dell'evoluzione della riflessione a livello nazionale ed europeo

Fondamenti di liceità del trattamento

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea 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 privacy - d.lgs. 196/2003 (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).

In particolare:

Consenso

COSA CAMBIA

- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).
- Non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) 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.

COSA NON CAMBIA

- Deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).
- Deve essere manifestato attraverso “dichiarazione o azione positiva inequivocabile” (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Raccomandazioni

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

In particolare, occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all’interessato (art. 7.2), per esempio all’interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20).

Interesse vitale di un terzo

COSA CAMBIA

- Si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46).

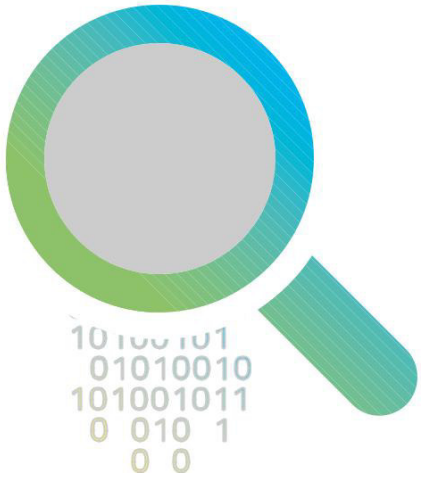
Interesse legittimo prevalente di un titolare o di un terzo

COSA CAMBIA

- Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso titolare; si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal nuovo pacchetto protezione dati.

COSA NON CAMBIA

- L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.
- Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.



Raccomandazioni

Il regolamento offre alcuni criteri per il bilanciamento in questione (si veda considerando 47) e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo “Articolo 29” sul punto (WP217).

Si confermano, inoltre, nella sostanza, i requisiti indicati dall’Autorità nei propri provvedimenti in materia di bilanciamento di interessi (si veda, per esempio, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992 con riguardo ad alcune tipologie di trattamento di dati biometrici; http://www.garanteprivacy.it/web/guest/home/docweb/-/ docweb-display/docweb/1712680 con riguardo all’utilizzo della videosorveglianza;http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6068256 in merito all’utilizzo di sistemi di rilevazione informatica anti-frode; ecc.) con particolare riferimento agli esiti delle verifiche preliminari condotte dall’Autorità, con eccezione ovviamente delle disposizioni che il regolamento ha espressamente abrogato (per esempio: obbligo di notifica dei trattamenti). I titolari dovrebbero condurre la propria valutazione alla luce di tutti questi principi.

Informativa

Contenuti dell’informativa

COSA CAMBIA

- I contenuti dell’informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest’ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).
- 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.
- Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l’informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l’interessato.

Tempi dell'informativa

- Nel caso di dati personali non raccolti direttamente presso l'interessa-to (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa

- Il regolamento specifica molto più in dettaglio rispetto al Codice le caratte-ristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).
- L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

- Sono inoltre parzialmente diversi i requisiti che il regolamento fissa per l'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, di quest'ultimo), anche se occorre sottolineare che spetta 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 (si veda art. 14, paragrafo 5, lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

- L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato prima di effettuare la raccolta dei dati

  (se raccolti direttamente presso l'interessato – art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

NOTA: ogni volta che le finalità cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

Raccomandazioni

È opportuno che i titolari di trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da apportare le modifiche o le integrazioni eventualmente necessarie prima del 25 maggio 2018.

Il regolamento supporta chiaramente il concetto di informativa "stratificata", più volte esplicitato dal Garante nei suoi provvedimenti (si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/

docweb/1712680 relativo all'utilizzo di un'icona specifica per i sistemi di video-sorveglianza con o senza operatore; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675 contenente prescrizioni analoghe rispetto all'utilizzo associato di sistemi biometrici e di videosorveglian-za in istituti bancari), in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove l'utilizzo di strumenti elettronici per garantire la massima diffusione e semplificare la prestazione delle informative.

I titolari potranno, dunque, una volta adeguata l'informativa nei termini sopra indicati, continuare o iniziare a utilizzare queste modalità per la prestazione dell' informativa, comprese le icone che l'Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.) – in attesa della definizione di icone standardizzate da parte della Commissione.
Dovranno essere adottate anche le misure organizzative interne idonee a garantire il rispetto della tempistica: il termine di 1 mese per l'informativa all'interessato è chiaramente un termine massimo, e occorre ricordare che l'art. 14, paragrafo 3, lettera a), del regolamento menziona in primo luogo che il termine deve essere "ragionevole".

Poiché spetterà al titolare valutare lo sforzo sproporzionato richiesto dall'in-formare una pluralità di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l'esistenza di specifiche disposizioni normative nei termini di cui all'art. 23, paragrafo 1, del regolamento, sarà utile fare riferimento ai criteri evidenziati nei provvedimenti con cui il Garante ha riconosciuto negli anni l'esistenza di tale sproporzione (si veda, in particolare, il provvedimento del 26 novembre 1998 – http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39624; più di recente, fra molti, http://www.garante-privacy.it/web/guest/home/docweb/-/docweb-display/docweb/3864423 in tema di esonero dagli obblighi di informativa).

Diritti degli interessati

Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

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

- Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. 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).

- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

- Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (art. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)).

- L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni (si veda il paragrafo "Cosa cambia"). Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6).

- 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).
  In questo senso, in via generale, possono continuare a essere applicate tutte le deroghe previste dall'art. 8, comma 2, del Codice in quanto compatibili con le disposizioni citate. Al riguardo, il Garante sta valutando la piena rispondenza delle disposizioni citate in tale articolo del Codice con i requisiti fissati per la legislazione nazionale dall'articolo 23, paragrafo 2, del regolamento.

Raccomandazioni

È opportuno che i titolari di trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto attualmente previsto – dovrà avere per impostazione predefinita forma scritta (anche elettronica). Potranno risultare utili le indicazioni fornite dal Garante nel corso degli anni con riguardo all'intelligibilità del riscontro fornito agli interessati e alla completezza del riscontro stesso (si vedano varie decisioni relative a ricorsi contenute nel Bollettino dell'Autorità pubblicato qui: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/ docweb/766652, e più recentemente, fra molti, http://www.garanteprivacy. it/web/guest/home/docweb/-/docweb-display/docweb/1449401 in materia di dati sanitari, ovvero http://www.garanteprivacy.it/web/guest/home/ docweb/-/docweb-display/docweb/1290018 in materia di dati telematici).

Quanto alla definizione eventuale di un contributo spese da parte degli interessati, che il regolamento rimette al titolare del trattamento, l'Autorità intende valutare l'opportunità di definire linee-guida specifiche (anche sul fondamento delle determinazioni assunte sul punto nel corso degli anni: si veda in particolare la Deliberazione n. 14 del 23 dicembre 2004 - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/ docweb/1104892 , di concerto con le altre autorità Ue, alla luce di quanto prevede l'art. 70 del regolamento con riguardo ai compiti del Board.

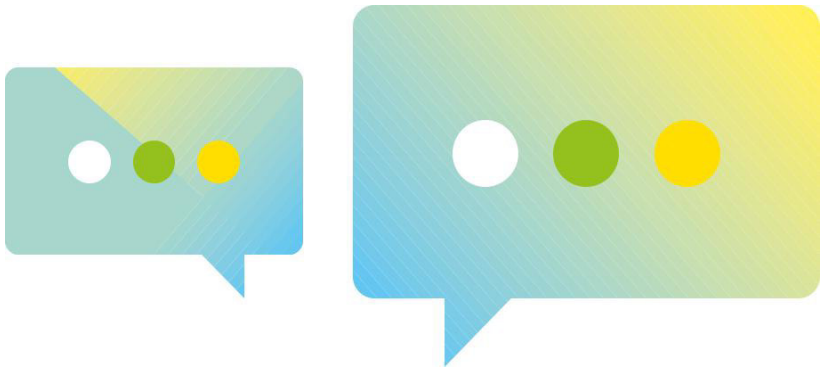
Diritto di accesso (art. 15)

COSA CAMBIA

- Il diritto di accesso prevede in ogni caso 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 occorre 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.

Raccomandazioni

- Oltre al rispetto delle prescrizioni relative alla modalità di esercizio di que-sto e degli altri diritti (si veda “Modalità per l’esercizio dei diritti”), i titolari possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali (si veda considerando 68).

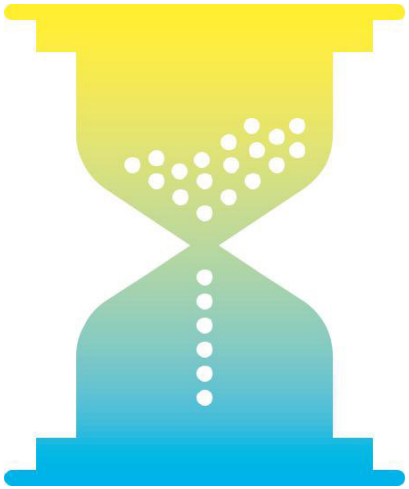


Diritto di cancellazione (diritto all'oblio) (art.17)

COSA CAMBIA

- Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazio-ne dei propri dati personali in forma rafforzata.
  Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).

- Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la can-cellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).



Diritto di limitazione del trattamento (art. 18)

- Si tratta di un diritto diverso e più esteso rispetto al “blocco” del trattamento di cui all’art. 7, comma 3, lettera a), del Codice: in particola-re, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l’interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell’art. 21 del regolamento (in attesa della valutazione da parte del titolare).

- Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (con-senso dell’interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Raccomandazioni

Il diritto alla limitazione prevede che il dato personale sia “contrassegnato” in attesa di determinazioni ulteriori; pertanto, è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Diritto alla portabilità dei dati (art. 20)

COSA CAMBIA

- Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

- Non si applica ai trattamenti non automatizzati (quindi non si applica agli 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 (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pub-blico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare (si veda il considerando 68 per maggiori dettagli).

- Inoltre, il titolare deve essere in grado di trasferire direttamente i dati por-tabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Raccomandazioni

Il Gruppo "Articolo 29" ha pubblicato recentemente linee-guida speci-fiche dove sono illustrati e spiegati i requisiti e le caratteristiche del dirit-to alla portabilità con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilità (http://ec.europa.eu/newsroom/docu-ment.cfm?doc_id=44099 con le relative FAQ http://ec.europa.eu/informa-tion_society/newsroom/image/document/2016-51/wp242_annex_en_40854. pdf; versione italiana per adesso disponibile sul sito del Garante: http:// www.garanteprivacy.it/garante/document?ID=6058842 con le relative FAQ

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058857).

Al riguardo, si ricordano i numerosi provvedimenti con cui l'Autorità ha indicato criteri per il bilanciamento fra i diritti e le libertà fondamentali di terzi e quelli degli interessati esercitanti i diritti di cui all'art. 7 del Codice (si vedano, fra molti, http://www.garanteprivacy.it/web/guest/home/ docweb/-/docweb-display/docweb/3251012 e, con riguardo all'attività ban-caria in generale, http://www.garanteprivacy.it/web/guest/home/docweb/-/ docweb-display/docweb/1457247).
Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzi-no formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un formato interoperabile secondo le indicazioni fornite nel considerando 68 e nelle linee-guida del Gruppo "Articolo 29".

Titolare, responsabile, incaricato del trattamento

Il regolamento:

COSA CAMBIA

- disciplina la contitolarità del trattamento (art. 26) e impone 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, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

- fissa più dettagliatamente (rispetto all'art. 29 del Codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attri-buendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve 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 o dei trattamenti assegnati, le categorie di dati oggetto di 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;

- consente la nomina di sub-responsabili del trattamento da parte di un re-sponsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabi-le primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3);

- prevede obblighi specifici 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 desi-gnazione 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 regolamento – diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice.

- Il regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice italiano. Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 Codice), il regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento).

Raccomandazioni

I titolari di trattamento dovrebbero valutare attentamente l'esistenza di eventuali situazioni di contitolarità (si vedano, in proposito, le indicazioni fornite dal Garante in vari provvedimenti, fra cui http://www.garantepri-vacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785), essendo obbligati in tal caso a stipulare l'accordo interno di cui parla l'art. 26, paragrafo 1, del regolamento. Sarà necessario, in particolare, individuare il "punto di contatto per gli interessati" previsto dal suddetto articolo ai fini dell'esercizio dei diritti previsti dal regolamento.

I titolari di trattamento dovrebbero verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsa-bili siano conformi a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del regolamento. Dovranno essere apportate le necessarie integrazio-ni o modifiche entro il 25 maggio 2018, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti. La Commissione
e le autorità nazionali di controllo (fra cui il Garante) stanno valutando la definizione di clausole contrattuali modello da utilizzare a questo scopo.

Attraverso l'adesione a codici deontologici ovvero l'adesione a schemi di cer-tificazione il responsabile può dimostrare le "garanzie sufficienti" di cui all'art. 28, paragrafi 1 e 4. Il Garante sta valutando i codici deontologici attualmente vigenti per alcune tipologie di trattamento nell'ottica dei requisiti fissati nel regolamento (art. 40), mentre per quanto concerne gli schemi di certificazio-ne occorrerà attendere anche l'intervento del legislatore nazionale che dovrà stabilire alcune modalità di accreditamento dei soggetti certificatori (se diversi dal Garante: si veda art. 43). In ogni caso, il Gruppo "Articolo 29" sta lavorando sui temi e sarà opportuno tenere conto degli sviluppi che inter-verranno in materia nei prossimi mesi.

Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di “responsabilizzazione” di titolari e respon-sabili del trattamento che prevede l’adozione di misure atte a garantire proat-tivamente l’osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante (si veda art. 30 del Codice e, fra molti, http://www.garanteprivacy.it/web/guest/ home/docweb/-/docweb-display/docweb/1507921, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1508059 per quanto riguarda la pubblica amministrazione, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953 in materia di tracciamento delle attività bancarie) in quanto misure atte a garantire e dimostrare “che il trattamento è effettuato confor-memente” al regolamento (si veda art. 24, paragrafo 1, del regolamento).

Approccio basato sul rischio e misure di accountability di titolari e responsabili

COSA CAMBIA

- Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamen-to (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affi-dato ai titolari il compito di decidere autonomamente le modalità, le garan-zie e i limiti del trattamento dei dati personali – nel rispetto delle disposizio-ni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

- Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" (si veda art. 25), ossia dalla necessità di configu-rare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e pro-prio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del rego-lamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifi-che e dimostrabili.

- Fondamentali fra tali attività sono quelle connesse al secondo criterio indivi-duato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio

di impatti negativi sulle libertà e i diritti degli interessati (si vedano conside-rando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano 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 ini-ziare il trattamento (avendo adottato le misure idonee a mitigare sufficien-temente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità 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 autonoma-mente 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/respon-sabile 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 è chiamato, infatti,

  a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si rende-ranno necessari alla luce dello sviluppo delle tecnologie e dei sistemi
  di trattamento dati.

Si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati recentemente pubblicate dal Gruppo “Articolo 29”, disponibili qui: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

Nei paragrafi seguenti si richiamano alcune delle principali novità in termini di adempimenti da parte di titolari e responsabili del trattamento.

Registro dei trattamenti

COSA CAMBIA

- Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all’art. 30. Si tratta di uno strumen-to fondamentale non soltanto ai fini dell’eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trat-tamenti in essere all’interno di un’azienda o di un soggetto pubblico – indi-spensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Raccomandazioni

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a pre-scindere dalle dimensioni dell’organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un’accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.

I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trat-tamenti svolti.

Nello specifico, si richiama l'attenzione sulla sostanziale coincidenza fra i con-tenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolamento; l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni.

Misure di sicurezza

COSA CAMBIA

- Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al ti-tolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazio-ne per attestare l'adeguatezza delle misure di sicurezza adottate.
  Tuttavia, facendo anche riferimento alle prescrizioni contenute, in partico-lare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, para-grafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il

caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pub-blici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Notifica delle violazioni di dati personali

COSA CAMBIA

- A partire dal 25 maggio 2018, tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifi-ca all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordina-ta alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle vio-lazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno ecce-zione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento. Su questo e su tutta la disciplina in materia, il Comitato europeo della protezione dati (si veda art. 70, paragrafo 1, lettere g) e h)) è chiamato a formulare linee-guida specifiche, alle quali sta già lavorando il Gruppo "Articolo 29". Si ricorda, inoltre, che l'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico (si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835) che intende rielaborare al fine di renderlo utilizzabile da tutti i titolari di trattamento secondo quanto prevede il regolamento.

Raccomandazioni

Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i prov-vedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice.
Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale docu-mentazione, su richiesta, al Garante in caso di accertamenti.

Responsabile della protezione dei dati

COSA CAMBIA

- Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approc-cio responsabilizzante che è proprio del regolamento (si veda art. 39), essen-do finalizzata a facilitare l'attuazione del regolamento da parte del titolare/ responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sen-sibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimen-to della valutazione di impatto di cui all'art. 35. La sua designazione è obbliga-toria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, compe-tenze manageriali: si vedano art. 38 e 39) in termini che Gruppo "Articolo 29" ha ritenuto opportuno chiarire attraverso alcune linee-guida di recente pubbli-cazione, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (si veda: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287).

Trasferimenti di dati verso Paesi terzi e organismi internazionali

COSA CAMBIA

- In primo luogo, viene meno il requisito dell'autorizzazione nazionale (si vedano art. 45, paragrafo 1, e art. 46, paragrafo 2). Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole con-trattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del regola-mento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto attualmente previsto dall'art. 44 del Codice.

  Tuttavia, l'autorizzazione del Garante sarà ancora necessaria se un titolare desidera utilizzare clausole contrattuali ad-hoc (cioè non rico-nosciute come adeguate tramite decisione della Commissione europea) oppure accordi amministrativi stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.

- 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 certifica-zione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. Tuttavia (si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2), tali tito-lari dovranno assumere, inoltre, un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento che sia giuridica-mente vincolante e azionabile dagli interessati.

- Il regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze ammini-strative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (si veda art. 48). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'art. 49. A tale riguardo, si deve ricorda-re che il regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto dell'Ue (si veda art. 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

- Il regolamento fissa i requisiti per l'approvazione delle norme vincolan-ti d'impresa e i contenuti obbligatori di tali norme. L'elenco indicato al riguardo nel paragrafo 2 dell'art. 47 non è esaustivo e, pertanto, potran-no essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza di cui agli artt. 63-65 del regolamento – ossia, è previsto in ogni caso l'intervento del Comitato europeo per la protezione dei dati (si veda art. 65, paragrafo 1, lettera d)).

- Il regolamento (si veda Capo V) ha confermato l'approccio attualmente vigente in base alla direttiva 95/46 e al Codice italiano per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

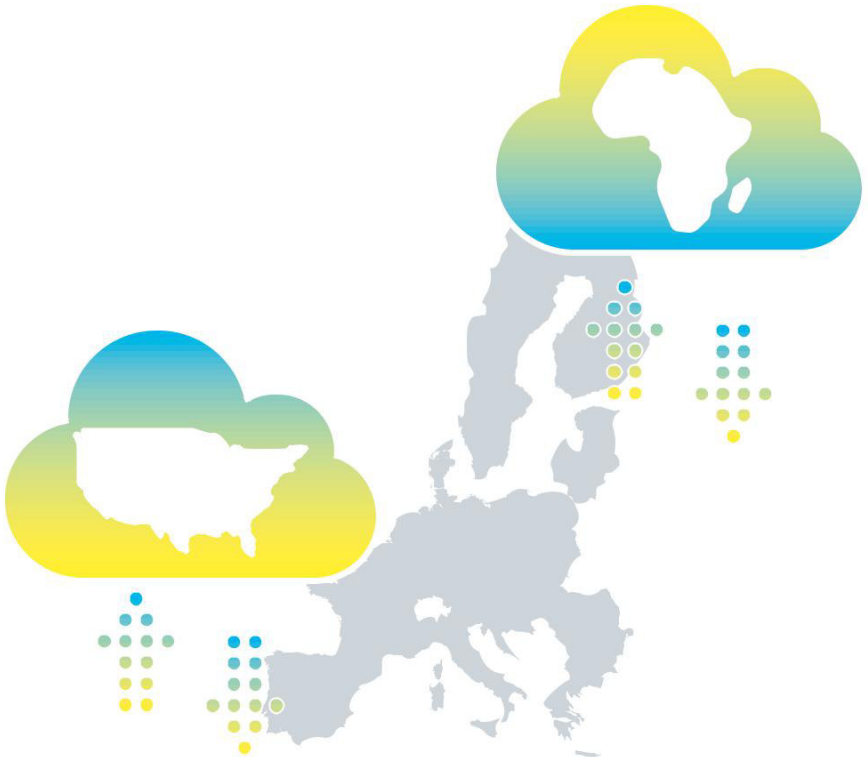
  i. adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea (si veda art. 44, comma 1, lettera b), del Codice);

  ii. in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere forni-te dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello) (si veda art. 44, comma 1, lettera a) del Codice);

  iii. in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (corrispondenti in parte alle disposizioni dell'art. 43, comma 1, del Codice).

- Le decisioni di adeguatezza sinora adottate dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica (si vedano art. 45, paragrafo 9, e art. 96). Restano valide, conseguente-mente, le autorizzazioni nazionali sinora emesse dal Garante successiva-mente a tali decisioni di adeguatezza della Commissione

(si veda http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-da-ti-verso-paesi-terzi#1). Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi (si veda art. 46, paragrafo 5), sino a loro eventuale modifica.



NOTE

NOTE

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

VERTIGO DESIGN

Piazza di Monte Citorio, 121
00186 Roma
Tel: +39-06-696771
Fax: +39-06-696773785
www.garanteprivacy.it

Antonello Soro, Presidente
Augusta Iannini, Vice Presidente
Giovanna Bianchi Clerici, Componente
Licia Califano, Componente

Giuseppe Busia, Segretario generale

Per informazioni presso l'Autorità:
Ufficio per le relazioni con il pubblico
lunedì - venerdì ore 10.00 - 12.30
tel. 06 696772917
e-mail: urp@gpdp.it

Pubblicazione a cura
del Servizio relazioni esterne e media

Stampa: Ugo Quintily Spa - luglio 2017 - Prima edizione