Doveri e responsabilità*


Stampa


Invia per mail


Condividi

Tutti possono liberamente raccogliere, per uso strettamente personale o domestico, dati personali riguardanti altri individui, e quindi senza una connessione con un'attività commerciale o professionale (esempio: i dati raccolti per uso personale nelle proprie agende cartacee o elettroniche)

Quando però i dati sono raccolti e utilizzati per altre finalità (ad esempio, un'azienda che vuole vendere prodotti, un professionista che vuole pubblicizzare i suoi servizi, un'associazione che vuole trovare nuovi iscritti, un partito che fa propaganda politica, ecc.), il trattamento dei dati personali deve rispettare alcune regole.

Informativa

Fatte salve alcune eccezioni, chi intende effettuare un trattamento di dati personali deve prima fornire all'interessato alcune informazioni (articolo 13 del Regolamento UE 2016/679) per metterlo nelle condizioni di esercitare i propri diritti (articoli 15-22 del Regolamento medesimo).

In particolare, l'informativa deve spiegare:

a) per quale scopo e la base giuridica sulla quale si fonda il trattamento dei dati personali;

b) se il conferimento dei dati personali è obbligatorio o facoltativo;

c) le conseguenze di un eventuale rifiuto a rendere disponibili i dati personali;

d) a chi saranno comunicati o se saranno saranno trasferiti all'estero i dati personali;

e) i diritti previsti dagli articoli 11-22 del Regolamento (UE) 2016/679;

f) chi è il titolare e (se è stato designato) il responsabile del trattamento;

g) gli eventuali legittimi interessi del titolare, se questi costituiscono il fondamento di liceità del trattamento;

h) il periodo di conservazionie dei dati e il diritto di revocare il consenso;

i) l'esistenza di un processo decisionale automatizzato;

l) l'origine dei dati, se raccolti presso terzi.

Se i dati personali sono stati raccolti da altre fonti (ad esempio, archivi pubblici, familiari dell'interessato, ecc.), cioè non direttamente presso l'interessato, l'informativa deve essere resa:

- quando i dati sono registrati

oppure

- non oltre la prima comunicazione a terzi

L'omessa o inidonea informativa è punita con la sanzione amministrativa pecuniaria stabilita dall'articolo 83, paragrafo 5, lett. b), del Regolamento (UE) 2016/679.

Consenso

Soggetti privati

Fatte salve alcune specifiche eccezioni, per i soggetti privati il trattamento di dati personali è possibile con il consenso inequivocabile dell'interessato. Il titolare deve sempre essere in grado di dimostrare che l'interessato ha prestato il proprio consenso (articolo 7 del Regolamento UE 2016/679), che è valido se:

- all'interessato è stata resa l'informazione (articoli 12 e 13 del Regolamento);
- è stato espresso dall'interessato liberamente e può essere sempre revocabile;
- è stato espresso esplicitamente, per una o più finalità specifiche, qualora il trattamento abbia ad oggetto categorie particolari di dati personali.

Il trattamento di dati personali effettuato in assenza del consenso è punito con la sanzione amministrativa pecuniaria stabilita dall'articolo 83, paragrafo 5, lett. a), del Regolamento (UE) 2016/679.

Soggetti che trattano dati personali adempiere un obbligo legale, per eseguire un compito di interesse pubblico o per l'esercizio di pubblici poteri

I predetti soggetti non devono richiedere il consenso dell'interessato, purché il trattamento sia effettuato per il perseguimento dei menzionati presupposti di legittimità che qualificano i titolari medesimi (articolo 6, paragrafo 1, lett. c ed e del Regolamento UE 2016/679).

Il trattamento di dati personali effettuato in violazione dell' articolo 6, paragrafo 1, lett. c) ed e) è punito con la sanzione amministrativa pecuniaria stabilita dall'articolo 83, paragrafo 5, lett. a), del Regolamento (UE) 2016/679.

Modalità del trattamento

Il trattamento deve avvenire nel rispetto dei seguenti principi (articolo 5 del Regolamento UE 2016/679):

- liceità, correttezza e trasparenza del trattamento;
- finalità del trattamento;
- esattezza e aggiornamento dei dati;
- adeguatezza, pertinenza, e limitazione dei dati raccolti rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati trattati;
- conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- sicurezza adeguata del trattamento.

Il trattamento di dati personali effettuato in violazione dell' articolo 5, è punito con la sanzione amministrativa pecuniaria stabilita dall'articolo 83, paragrafo 5, lett. a), del Regolamento (UE) 2016/679.

Misure di sicurezza

Il titolare del trattamento, anche in base al principio di responsabilizzazione, è obbligato ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio di distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato che potrebbero cagionare un danno fisico, materiale o immateriale (articolo 32 del Regolamento UE 2016/679).

In particolare, il titolare deve adottare, se del caso, la pseudonimizzazione e la cifratura dei dati; misure pe garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; il tempestivo ripristino della disponibilità dei dati; procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

L'omessa applicazione delle misure di sicurezza è punita, a seconda dei casi, con la sanzione amministrativa pecuniaria stabilita dall'articolo 83, paragrafo 4, lett. a), ovvero paragrafo 5, lett. a), del Regolamento (UE) 2016/679.

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali – cioè la violazione dei sistemi di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati – il titolare del trattamento deve notificare l'evento al Garante entro 72 ore dal momento in cui ne è venuto a conoscenza.

Quando la violazione è suscettibile di presentare un rischio elevato per le persone fisiche, a dseterminate condizioni, il titolare deve comunicare l'evento all'interessato senza ingiustificato ritardo (articoli 33 e 34 del Regolamento UE 2016/679).

Il mancato rispetto degli obblighi di notifica è punito con la sanzione amministrativa pecuniaria stabilita dall'articolo 83, paragrafo 4, lett. a), del Regolamento (UE) 2016/679.

Nel caso in cui il trattamento dei dati personali, allorchè prevede in particolare l'uso di nuove tecnologie e, pur non coinvolgendo dati sensibili o dati giudiziari, presenti un rischio elevato per i diritti e le libertà fondamentali delle persone fisiche, il titolare prima di procedere al trattamento deve effettuare una valutazione di impatto (articolo 35 del Regolamento UE 2016/679). La valutazione di impatto deve esere effettuata, in particolare, nei seguenti casi:

- qualora venga effettuata una valutazione sistematica e globale di aspetti relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione;il trattamento si svolga su larga scala e abbia ad oggetto categorie particolari di dati personali o di dati relativi a condanne penali e reati;
- il trattamento consista nella sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Valutazione di impatto

Nel caso in cui la valutazione di impatto riveli che il trattamento presenterebbe un rischio elevato in assenza di adeguate misure volte ad attenuare il rischio adottate dal titolare, quest'ultimo è tenuto a consultare il Garante per la protezione

dei dati personali, affinchè fornisca un parere scritto (articolo 36 del Regolamento UE 2016/679).

Il trattamento di dati personali effettuato in violazione degli articoli 35 e 36 è punito con la sanzione amministrativa pecuniaria stabilita dall'articolo 83, paragrafo 4, lett. a), del Regolamento (UE) 2016/679.

TRATTAMENTO DI PARTICOLARI CATEGORIE DI DATI PERSONALI E DI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

Particolari categorie di dati personali

Il trattamento di tale tipologia di dati personali è consentito quando:

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato.

Inoltre, i predetti tipi di dati personali possono essere lecitamente trattati quando il relativo utilizzo è necessario per:

- assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
- finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- motivi di interesse pubblico nel settore della sanità pubblica.
- il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Dati personali relativi a condanne penali e reati

Il trattamento di tale tipologia di dati personali è consentito soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione europea o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

TRASFERIMENTO DEI DATI ALL'ESTERO

Verso Paesi appartenenti all'Unione europea

Le legislazioni dei Paesi aderenti all'Unione europea sono considerate equivalenti in relazione all'adeguata tutela in materia di protezione dei dati personali. Il trasferimento attraverso o verso questi Paesi non è quindi soggetto a particolari restrizioni.

Verso Paesi non appartenenti all'Unione europea

Il trasferimento di dati personali verso Paesi non appartenenti all'Unione europea è possibile quando intervengano le seguenti specifiche garanzie (articoli da 44 a 49 del Regolamento UE 2016/679):

a) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;

b) 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 tipo);

c) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

Sono altresì vietati trasferimenti 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, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (articolo 48 del Regolamento UE 2016/679). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'articolo 49 del Regolamento medesimo. E' 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'Unione europea (articolo 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

Il trattamento di dati personali effettuato in violazione degli articoli da 44 a 49 è punito con la sanzione amministrativa pecuniaria stabilita dall'articolo 83, paragrafo 5, lett. c), del Regolamento (UE) 2016/679.

- Vedi anche la sezione del sito dedicata al tema

CESSAZIONE DEL TRATTAMENTO

In caso di cessazione del trattamento, i dati personali devono essere *(art. 5, par. 1. lett. b, del Regolamento)*:

a) distrutti o cancellati;

b) trattati a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o statistici.

(Scheda di sintesi redatta dall'Ufficio del Garante a mero scopo divulgativo. Per un quadro completo della materia, si rimanda alla legislazione in tema di protezione dei dati personali e ai provvedimenti dell'Autorità. Per dubbi e domande si suggerisce di contattare l'Urp del Garante)