Doveri - Come trattare correttamente i dati

(Schede di sintesi redatte 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)

Principi generali del trattamento di dati personali

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, che qui si ricordano brevemente:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Il Regolamento (articolo 5, paragrafo 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione" (o accountability) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate **per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento."**

Assicurare la liceità del trattamento di dati personali

Il Regolamento, come già previsto dal Codice in materia di protezione dei dati personali, prevede che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del Regolamento:

- 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.

Per quanto riguarda le **"categorie particolari di dati personali"** (articolo 9 del Regolamento), il loro trattamento è vietato, in prima battuta, a meno che il titolare possa dimostrare di soddisfare almeno una delle condizioni fissate all'articolo 9, paragrafo 2 del Regolamento, che qui ricordiamo:

- 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;
- il trattamento è necessario per uno dei seguenti scopi:

- 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;
- per 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;
- per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
- per 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;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Per alcune di tali finalità sono previste limitazioni o prescrizioni ulteriori, anche nel diritto nazionale.

Consenso

Quando il trattamento si fonda sul consenso dell'interessato, il titolare deve sempre essere in grado di dimostrare (articolo 7.1 del Regolamento) che l'interessato ha prestato il proprio consenso), che è valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali (articoli 13 o 14 del Regolamento);
- è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre revocabile.

Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (articolo 7.2), per esempio all'interno della modulistica.

Non è ammesso il consenso tacito o presunto (per esempio, presentando caselle già spuntate su un modulo).

Quando il trattamento riguarda le "categorie particolari di dati personali" (articolo 9 Regolamento) il consenso deve essere "esplicito"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – articolo 22).

Il consenso 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 le categorie particolari di dati di cui all'articolo 9 Regolamento).

Per approfondimenti: Linee-guida del WP29 sul consenso, qui disponibili: www.garanteprivacy.it/regolamentoue/consenso. Si segnalano anche le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy/regolamentoue/profilazione.

Interesse vitale di un terzo

Si può invocare tale base giuridica per il trattamento di dati personali solo se nessuna delle altre condizioni di liceità può trovare applicazione (considerando 46).

Interesse legittimo prevalente di un titolare o di un terzo

Il ricorso a questa base giuridica per il trattamento di dati personali presuppone che il titolare stesso effettui un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato. Dal 25 maggio 2018, dunque, tale bilanciamento non spetta più all'Autorità, in linea di principio. Si tratta di una delle principali espressioni del principio di " responsabilizzazione" introdotto dal Regolamento (UE) 2016/679.

L’interesse legittimo del titolare o del terzo deve risultare prevalente 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.

Si ricordi, inoltre, che il legittimo interesse non può essere invocato isolatamente quale base giuridica per il trattamento delle categorie particolari di dati personali (articolo 9, paragrafo 2, del Regolamento).

Trasparenza del trattamento: l’informativa agli interessati

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

QUANDO

L’informativa (disciplinata nello specifico dagli artt. 13 e 14 del Regolamento) deve essere fornita all’interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati (se raccolti direttamente presso l’interessato: articolo 13 del Regolamento).

Nel caso di dati personali non raccolti direttamente presso l’interessato (articolo 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 prevedeva l’articolo 13, comma 4, del Codice).

COSA

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.). Se i dati non sono raccolti direttamente presso l’interessato (articolo 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.

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.

COME

L’informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: articolo 12, paragrafo 1, e considerando 58). Sono comunque ammessi “altri mezzi”, quindi può essere fornita anche in forma orale, ma nel rispetto delle caratteristiche di cui sopra (articolo 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 estesa (articolo 12, paragrafo 7); queste icone in futuro dovranno essere uniformate in tutta

l'Ue attraverso l'intervento dalla Commissione europea.

In base al Regolamento, si deve porre particolare attenzione alla formulazione dell'informativa, che deve essere soprattutto comprensibile e trasparente per l'interessato, attraverso l'uso di un linguaggio chiaro e semplice. In particolare, bisogna ricordare che per i minori si devono prevedere informative idonee (anche considerando 58).

Per maggiori dettagli ed esempi di redazione di informative, il documento del WP29 in materia di "Trasparenza" del trattamento, qui disponibile: www.garanteprivacy.it/regolamentoue/trasparenza

Un approccio responsabile al trattamento: Accountability

Il Regolamento pone l'accento sulla "responsabilizzazione" 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 Regolamento** (artt. 23-25, in particolare, e l'intero Capo IV del Regolamento). Dunque, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni 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" (articolo 25), ossia dalla necessità di configurare 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 proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto previsto dall'articolo 25, paragrafo 1, del Regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato 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 (considerando 75-77); 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 (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/Regolamentoue/DPIA). (Vedi anche: il tutorial del Garante sul concetto di "rischio")

All'esito di questa valutazione di impatto, il titolare:

- potrà decidere se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero, se il rischio risulta ciononostante elevato;
- dovrà consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità avrà quindi il compito di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58 del Regolamento (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

In conseguenza dell'applicazione del principio di accountability, dal 25 maggio 2018 non sono più previste

- la notifica preventiva dei trattamenti all'autorità di controllo;
- una verifica preliminare da parte del Garante per i trattamenti "a rischio" (anche se potranno esservi alcune eccezioni legate a disposizioni nazionali, previste in particolare dall'articolo 36, paragrafo 5 del Regolamento).

Al loro posto, il Regolamento prevede in capo ai titolari l'obbligo (pressoché generalizzato) di tenere un registro dei trattamenti e, appunto, di effettuare valutazioni di impatto in piena autonomia con eventuale successiva consultazione dell'Autorità.

Principio di "responsabilizzazione" dei titolari e responsabili del trattamento: principali elementi

Rapporti contrattuali fra titolare e responsabile del trattamento

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 privacy italiano.

Tuttavia, il Regolamento (articolo 28) prevede dettagliatamente le caratteristiche **dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli 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'articolo 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

Inoltre, il Regolamento prevede **obblighi specifici in capo ai responsabili del trattamento, distinti da quelli pertinenti ai rispettivi titolari**. Ciò riguarda, in particolare:

- la tenuta del registro dei trattamenti svolti (articolo 30, paragrafo 2);
- l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (articolo 32);
- la designazione di un RPD-DPO, nei casi previsti dal Regolamento o dal diritto nazionale (articolo 37).

Una novità importante del Regolamento è la possibilità di designare sub-responsabili del trattamento da parte di un responsabile (articolo 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile 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" (articolo 82, paragrafo 1 e paragrafo 3).

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti - ma solo se non effettuano trattamenti a rischio (articolo 30, paragrafo 5) - **devono tenere un registro delle operazioni di trattamento**, i cui contenuti sono indicati all'articolo 30.

Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. I contenuti del registro sono fissati nell'articolo 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 trattamenti svolti.

Il registro deve avere **forma scritta**, anche elettronica, e deve essere esibito su richiesta al Garante.

Misure di sicurezza

Il titolare del trattamento, come pure il responsabile del trattamento, è obbligato ad adottare misure tecniche e organizzative **idonee a garantire un livello di sicurezza adeguato al rischio del trattamento** (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Fra tali misure, il Regolamento menziona, in particolare, la pseudonimizzazione e la cifratura dei dati; misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; misure atte a garantire il tempestivo ripristino della disponibilità dei dati; procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

La lista di cui al paragrafo 1 dell'articolo 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per questi motivi, non possono sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure “minime” di sicurezza poiché tale valutazione è rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del Regolamento.

Vi è, inoltre, la possibilità di utilizzare l’adesione a specifici codici di condotta o a schemi di certificazione per attestare l’adeguatezza delle misure di sicurezza adottate (articolo 32, paragrafo 3).

Notifica di una violazione dei dati personali

A partire dal 25 maggio 2018, tutti i titolari dovranno notificare al Garante le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque “senza ingiustificato ritardo”, se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (considerando 85). Pertanto, la notifica all’Autorità dell’avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre “senza ingiustificato ritardo”; fanno eccezione le circostanze indicate al paragrafo 3 dell’articolo 34.

I contenuti della notifica all’Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli articolo 33 e 34 del Regolamento.

Tutti i titolari di trattamento devono 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 provmenti adottati (articolo 33, paragrafo 5). È bene, dunque, adottare le misure necessarie a documentare eventuali violazioni, anche perché i titolari sono tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy/regolamentoue/databreach.

Responsabile della protezione dei dati

La designazione di un “responsabile della protezione dati” (RPD) è finalizzata a facilitare l’attuazione della normativa da parte del titolare/responsabile (articolo 39). Non è un caso, infatti, che fra i compiti del RPD rientrino “la sensibilizzazione e la formazione del personale” e la sorveglianza sullo svolgimento della valutazione di impatto di cui all’articolo 35, oltre alla funzione di punto di contatto per gli interessati e per il Garante rispetto a ogni questione attinente l’applicazione del Regolamento.

La sua designazione è obbligatoria in alcuni casi (articolo 37), e il Regolamento delinea le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: articoli 38 e 39) in termini che il Gruppo di lavoro “Articolo 29” ha ritenuto opportuno chiarire attraverso alcune linee-guida, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (www.garanteprivacy.it/Regolamentoue/rpd).

Si segnalano anche i materiali disponibili nella sezione “Responsabile della protezione dati” sul sito del Garante, che comprendono ulteriori FAQ sul punto (www.garanteprivacy/regolamentoue/rpd)

I diritti degli interessati

I titolari del trattamento devono rispettare le modalità previste per l’esercizio di tutti i diritti da parte degli interessati, stabilite, in via generale, negli artt. 11 e 12 del Regolamento

- In primo luogo, 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, il responsabile del trattamento è tenuto a collaborare con il titolare ai fini dell’esercizio di tali diritti (articolo 28, paragrafo 3, lettera e)).

- Il titolare ha il diritto di chiedere informazioni necessarie a identificare l’interessato, e quest’ultimo ha il dovere di fornirle,

secondo modalità idonee (, in particolare, articolo 11, paragrafo 2 e articolo 12, paragrafo 6).

- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), pari a 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.

- 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.

- 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 (articolo12, paragrafo 5) - ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (articolo 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 (articolo 12, paragrafo 1; articolo 15, paragrafo 3).

Trasferimento dei dati all'estero

- Vedi la sezione del sito dedicata al tema