GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GUIDA ALL'APPLICAZIONE DEL REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

EDIZIONE 2023

GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

IL COLLEGIO

Pasquale Stanzione
Presidente

Ginevra Cerrina Feroni
Vice Presidente

Agostino Ghiglia
Componente

Guido Scorza
Componente

www.gpdp.it

INDICE

INTRODUZIONE

Dalla liceità del trattamento all'informativa, dai diritti degli interessati al titolare del trattamento, fino alla responsabilizzazione del titolare e all'approccio basato sul rischio, la Guida intende offrire una panoramica sui principali aspetti che imprese e soggetti pubblici devono tenere presenti per dare piena applicazione al Regolamento europeo in materia di protezione dati (GDPR).

La pubblicazione contiene raccomandazioni e riferimenti alle Linee guida europee, oltre che rimandi, ove opportuno o necessario, alla legislazione nazionale (in particolare, riguardo ai trattamenti per finalità di interesse pubblico o in ottemperanza a obblighi di legge).

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

Ogni trattamento di dati personali deve trovare fondamento in un'idonea base giuridica. L'articolo 6 del Regolamento individua i seguenti **fondamenti di liceità del trattamento**: consenso dell'interessato, adempimento di obblighi contrattuali, obblighi di legge cui è soggetto il titolare, salvaguardia degli interessi vitali della persona interessata o di terzi, interesse pubblico o esercizio di pubblici poteri da parte del titolare, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

In particolare:

CONSENSO

- **Deve** essere, in tutti i casi, libero, specifico, informato e inequivocabile: **non** è ammesso il consenso tacito o presunto (ad esempio, no a caselle pre-spuntate su un modulo).

- **Deve** essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano i considerando 39 e 42 del Regolamento).

- **Non** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è una modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i "dati sensibili"). Inoltre, il titolare (art. 7, par. 1) **deve** essere in grado di dimostrare che l'interessato abbia prestato il consenso a uno specifico trattamento.

- **Il consenso dei minori** è valido, in Italia, **a partire dai 14 anni** (in conformità con la normativa nazionale): prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

- Per quanto riguarda le categorie particolari di dati personali (art. 9), i cosiddetti "dati sensibili", il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione (art. 22) **[1]**.

1 Si segnalano, al riguardo, le Linee guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.gpdp.it/regolamentoue/profilazione

RACCOMANDAZIONI

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 della modulistica. Occorre poi prestare attenzione alla formula utilizzata per chiedere il consenso che deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (per maggiori approfondimenti si vedano le Linee guida 5/2020 del Comitato europeo per la protezione dei dati (EDPB) sul consenso, anche rispetto alla prestazione del consenso da parte di minori).

INTERESSE VITALE DI UN TERZO

- Si può invocare tale base giuridica solo nel caso in cui nessuna delle altre condizioni di liceità trovi applicazione (considerando 46 del GDPR).

INTERESSE LEGITTIMO PREVALENTE DI UN TITOLARE O DI UN TERZO

- Il legittimo interesse del titolare o del terzo, per costituire un valido fondamento di liceità, deve prevalere sui diritti e le libertà fondamentali dell'interessato. Il titolare deve essere in grado di dimostrare che il trattamento sia necessario per il suo legittimo interesse.

- Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **è compito dello stesso titolare**: si tratta di una delle principali espressioni del **principio di "responsabilizzazione"** introdotto dal legislatore europeo (Approfondimento a pag. 29).

- Il Regolamento chiarisce espressamente che il legittimo interesse del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei propri compiti.

RACCOMANDAZIONI

Il Regolamento offre alcuni criteri per il bilanciamento in questione (considerando 47) e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto (WP217) e alle indicazioni fornite dalla Corte di giustizia dell'Ue in proposito (sentenze nelle cause C-13/16 e C-708/18).

I titolari dovrebbero condurre la propria valutazione alla luce di tutti questi principi.

INFORMATIVA

CONTENUTI DELL'INFORMATIVA

- I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, par. 1, e 14, par. 1, del Regolamento.
  In particolare, l'informativa **deve sempre** specificare:
  - i dati di contatto del titolare e del suo rappresentante (se esistente);
  - quelli del Responsabile della protezione dei dati (RPD o DPO, secondo l'acronimo inglese di Data Protection Officer) ove esistente;
  - finalità e base giuridica del trattamento;
  - qual è il suo legittimo interesse, se quest'ultimo costituisce la base giuridica del trattamento;
  - eventuali destinatari o categorie di destinatari;
  - se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: se si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; se si utilizzano norme vincolanti d'impresa, in inglese Binding Corporate Rules - BCR; se sono state inserite specifiche clausole contrattuali standard, ecc. Approfondimento a pag. 38).

CONTENUTI DELL'INFORMATIVA

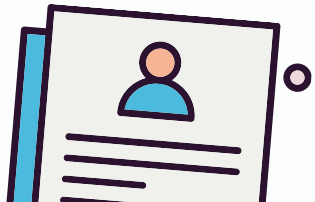
- Il Regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente". In particolare, il titolare deve specificare:
  - **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo;
  - la possibilità di revocare in qualsiasi momento il consenso al trattamento;
  - l'esistenza del diritto per l'interessato di chiedere l'accesso ai dati personali che lo riguardano, la rettifica, la cancellazione, la limitazione del trattamento o di opporsi allo stesso, nonché il diritto alla portabilità dei dati;
  - il diritto di **presentare un reclamo** a un'Autorità di controllo, che in Italia è il Garante per la protezione dei dati personali.

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

TEMPI DELL'INFORMATIVA

- L'informativa deve essere fornita all'interessato **prima di effettuare la raccolta dei dati**, se raccolti direttamente presso l'interessato (art. 13).
  Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14), 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).

- Se i dati non sono raccolti direttamente presso l'interessato (art. 14), 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, quali sono i destinatari dei dati**.



MODALITÀ DELL'INFORMATIVA

- Il Regolamento specifica anche le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio chiaro e semplice (art. 12, par. 1). Per i minori occorre prevedere informative idonee (considerando 58).
- L'informativa è data, **in linea di principio, per iscritto e preferibilmente in formato elettronico**, soprattutto nel contesto di servizi online (art. 12, par.1, e considerando 58), anche se sono ammessi "altri mezzi". Può essere quindi fornita anche oralmente, ma nel rispetto delle caratteristiche sopra indicate. Il Regolamento ammette inoltre l'utilizzo di **icone [2]** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** (art. 12, par. 7).

2 www.gpdp.it/informativechiare

In alcuni casi il Regolamento prevede che si possa fare a meno di un'informativa (art. 13, par. 4, e art. 14, par. 5, oltre a quanto previsto dall'art. 23, par. 1), 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 (**art. 14, par. 5, lett. b**).

RACCOMANDAZIONI

Il Regolamento supporta il concetto di **informativa "stratificata"**, in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi (il Garante per la protezione dei dati personali ha suggerito in questi anni vari modelli di icone nei suoi provvedimenti, per esempio in materia di videosorveglianza, banche, ecc.) che devono essere facilmente accessibili, e promuove **l'utilizzo di strumenti elettronici** per garantire la massima diffusione e semplificare la prestazione delle informative. Il Garante ha anche messo a disposizione sul proprio sito un data set di icone da poter utilizzare (www.gpdp.it/informativechiare).

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, par. 3, lett. a, menziona in primo luogo che il **termine deve essere "ragionevole"**.

Poiché spetterà al titolare valutare lo **sforzo sproporzionato** richiesto dall'informare 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, par. 1, sarà utile fare riferimento alle Linee guida del WP29 e dell'EDPB in materia di trasparenza, che contengono numerosi esempi a tale proposito oltre a fornire indicazioni operative più generali.

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.

- **Per tutti i diritti il termine per la risposta è 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**.
- L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. **Spetta al titolare** valutare la complessità del riscontro all'interessato e **stabilire l'ammontare dell'eventuale contributo** da chiedere, ma soltanto se si tratta di richieste **manifestamente infondate, eccessive o anche ripetitive** (art.12, par. 5), o se sono chieste **più "copie" dei dati personali** nel caso del diritto di accesso (art. 15, par. 3). In quest'ultima ipotesi, 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 lo richiede lo stesso interessato** (art. 12, par. 1, e art. 15, par. 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 (artt. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, par. 3, lett. 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 (si vedano, in particolare, art. 11, par. 2 e art. 12, par. 6).

- Sono ammesse **deroghe ai diritti** riconosciuti dal Regolamento, ma solo sul fondamento di disposizioni normative nazionali (art. 23) e ambiti specifici: diritto alla cancellazione/"oblio" (art. 17, par. 3); trattamenti effettuati a scopi giornalistici (art. 85); trattamenti a fini di ricerca scientifica, storica o di statistica (art. 89).
  Per approfondimenti su tali deroghe **si vedano anche l'art. 2-*undecies* e l'art. 2-*duodecies* del Codice Privacy**.

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. Indicazioni utili sono contenute nelle Linee guida del WP29 e dell'EDPB in materia di trasparenza, nelle Linee guida in materia di portabilità dei dati, nelle Linee guida in materia di diritto all'oblio, nelle Linee guida in materia di diritto di accesso.

DIRITTO DI ACCESSO (ART. 15)

- Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **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 questo 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)

- Il cosiddetto diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.
  Si prevede, infatti, l'obbligo per i titolari che 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" (art. 17, par. 2).

- Da sottolineare che l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (art. 17, par.1).

DIRITTO DI LIMITAZIONE DEL TRATTAMENTO (ART. 18)

- Il diritto di limitare (ossia, bloccare) il trattamento è esercitabile **non solo in caso di violazione** dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), **ma anche nel caso in cui l'interessato chieda 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 (consenso 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)

- 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":

  a) i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (tale diritto quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio);

  b) i dati che siano stati "forniti" dall'interessato al titolare (considerando 68 per maggiori dettagli).

- Il titolare deve essere inoltre in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

RACCOMANDAZIONI

Il Gruppo "Articolo 29" ha pubblicato Linee guida specifiche dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto 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 (versione italiana con le relative FAQ qui disponibile: www.gpdp.it/regolamentoue/portabilita).

Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto devono adottare 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:

- definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento**, in linea con il precedente quadro normativo sia europeo che nazionale;

- 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), corrispondenti nella sostanza agli "incaricati del trattamento" previsti dalla precedente normativa;

- 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 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 par. 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 responsabile (art. 28, par. 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" (art. 82, par. 1, e par. 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 (art. 30, par. 2); l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti (art. 32); **la designazione di un RPD-DPO** (si segnalano, al riguardo, le Linee guida sui responsabili della protezione dei dati, adottate dal Gruppo "Articolo 29"), nei casi previsti dal Regolamento o dal diritto nazionale (art. 37).

RACCOMANDAZIONI

I titolari di trattamento dovrebbero valutare attentamente l'esistenza di eventuali situazioni di contitolarità, essendo obbligati in tal caso a stipulare l'accordo interno di cui parla l'art. 26. Sarà necessario, in particolare, individuare il "punto di contatto per gli interessati" 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 responsabili siano conformi a quanto previsto, in particolare, dall'art. 28, par. 3o. Dovranno essere apportate le necessarie integrazioni o modifiche, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti.

Attraverso l'adesione a codici deontologici ovvero l'adesione a schemi di certificazione il responsabile può dimostrare le "garanzie sufficienti" di cui all'art. 28, par. 1 e 4. Il Garante ha approvato alcuni codici deontologici conformi al GDPR presentati da associazioni di categoria, mentre per quanto concerne gli schemi di certificazione l'intervento del Garante ha consentito di definire i requisiti aggiuntivi per l'accreditamento degli organismi di certificazione e l'EDPB ha delineato i contenuti essenziali e i criteri per la valutazione, da parte delle autorità di protezione dati, degli schemi di certificazione conformi al GDPR.

Si consiglia di leggere le Linee guida EDPB sui concetti di titolare e responsabile del trattamento, che illustrano un'ampia casistica di situazioni e forniscono raccomandazioni concrete.

APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY DI TITOLARI E RESPONSABILI

- Il Regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability in inglese) di titolari e responsabili. La "responsabilizzazione" prevede l'**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). Spetta 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 criterio è sintetizzato dall'espressione inglese **"data protection by default and by design"** (art. 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 nel quale il trattamento viene svolto 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 l'art. 25, par. 1) e richiede, pertanto, un'analisi preventiva e un impegno da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili**. Il Comitato europeo per la protezione dei dati (EDPB) ha fornito indicazioni operative nelle Linee guida 4/2019 sull'articolo 25 "Protezione dei dati fin dalla progettazione e per impostazione predefinita" (adottate il 20 ottobre 2020), insieme ad alcune raccomandazioni rivolte a titolari e responsabili.

- 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 **[3]** in materia di

[3] www.gpdp.it/regolamentoue/dpia

valutazione di impatto sulla protezione dei dati del Gruppo "Articolo 29").

All'esito della valutazione di impatto, il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) o consultare il Garante 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, se necessario, adottare tutte le misure correttive previste dal Regolamento: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento (art. 58).

- Dunque, **l'intervento delle Autorità di controllo è principalmente "ex post"**, ossia successivo alle determinazioni assunte autonomamente dal titolare. In questo contesto, si collocano anche gli obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia con eventuale successiva consultazione dell'Autorità (tranne alcune specifiche situazioni di trattamento previste dall'art. 36, par. 5). Peraltro, alle Autorità di controllo e, in particolare, al Comitato europeo della protezione dei dati (EDPB) spetta il ruolo di garantire uniformità di approccio e di fornire ausili interpretativi e analitici, attraverso l'elaborazione di Linee guida e altri documenti di indirizzo, da aggiornare alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

*Nei paragrafi seguenti si richiamano i **principali adempimenti** da parte di titolari e responsabili del trattamento.*

REGISTRO DEI TRATTAMENTI

- Tutti i titolari e i responsabili del trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (art. 30, par. 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche 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**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito, su richiesta, al Garante per la protezione dei dati personali.

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 prescindere 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 trattamenti svolti. Si veda, sul punto, il documento del WP29 e dell'EDPB sull'obbligo di tenuta di un registro dei trattamenti e sull'applicazione delle eventuali deroghe a tale obbligo.

MISURE DI SICUREZZA

- Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, par. 1). Il Regolamento indica una **lista aperta e non esaustiva** ("tra le altre, se del caso"), poiché la valutazione è rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati (art. 32).

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta (art. 40) o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate (art. 42).

NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI

- **Tutti i titolari** devono notificare al Garante 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 (considerando 85). Pertanto, **la notifica all'Autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare.

  Se la probabilità di tale rischio è elevata, si dovranno informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo" (l'art. 34, par. 3 fornisce alcune eccezioni). **I contenuti della notifica** all'Autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli art. 33 e 34 del Regolamento**.

  Si segnalano, al riguardo, le Linee guida EDPB in materia di notifica delle violazioni di dati personali e quelle contenenti esempi in materia di notifica delle violazioni di dati personali **[4]**.

4 Linee guida 9/2022 in materia di notifica delle violazioni di dati personali (data breach)

RESPONSABILE DELLA PROTEZIONE DEI DATI

- Anche la designazione di un Responsabile della protezione dati (RPD), o DPO se si utilizza l'acronimo inglese Data Protection Officer, riflette l'approccio responsabilizzante del Regolamento (art. 39).

  Non è un caso che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto (art. 35). Il Regolamento stabilisce i casi in cui la designazione del Responsabile è obbligatoria (art. 37) e tratteggia le caratteristiche soggettive e oggettive di questa figura: indipendenza, autorevolezza, competenze manageriali (art. 38 e 39).

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 provvedimenti adottati (art. 33, par. 5).
Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.
Il Garante ha messo a disposizione un modello specifico per la notifica delle violazioni di dati personali unitamente ad alcuni strumenti di supporto per l'autovalutazione del rischio derivante dalla violazione (disponibili qui: servizi.gpdp.it/databreach/s/).

TRASFERIMENTI DI DATI VERSO PAESI TERZI E ORGANISMI INTERNAZIONALI

- **Il Regolamento** (Capo V) vieta il trasferimento di dati personali al di fuori della UE e dello Spazio economico europeo, in linea di principio, a meno che intervengano specifiche garanzie, elencate in ordine gerarchico:

  i. *adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea* (art. 45);

  ii. *in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari o dai responsabili coinvolti, fra cui le norme vincolanti d'impresa (art. 47) e clausole contrattuali standard (art. 46, par. 2 lett. c, e lett. d);*

  iii. *in assenza di decisioni di adeguatezza applicabili al trasferimento, o di altre garanzie adeguate, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (art. 49).*

- Il trasferimento di dati verso un Paese terzo "adeguato" ai sensi della decisione dalla Commissione europea, o sulla base di clausole contrattuali modello, adottate sempre dalla Commissione, o di norme vincolanti d'impresa, non richiede alcuna autorizzazione preventiva da parte del Garante. La Commissione europea ha adottato un set di clausole contrattuali standard **[5]** per i trasferimenti di dati.
  Tuttavia, l'autorizzazione del Garante sarà ancora necessaria se un titolare desidera utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure **accordi amministrativi stipulati tra autorità pubbliche** (una delle novità introdotte dal Regolamento). Rispetto a questi specifici accordi amministrativi fra soggetti pubblici, l'EDPB ha adottato Linee guida che ne delimitano i contenuti essenziali **[6]**.
- Il Regolamento consente di ricorrere anche a **codici di condotta o a schemi di certificazione** per dimostrare le "garanzie adeguate" previste dall'art. 46.

5 eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32021D0914&from=IT
6 "Linee guida 2/2020 sull'articolo 46, par. 2, lett. a, e par. 3, lett. b, del regolamento 2016/679 per i trasferimenti di dati personali tra autorità ed organismi pubblici del SEE e di paesi non appartenenti al SEE" - Adottate il 15 dicembre 2020

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**, nel caso questi disciplinino i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. **Tuttavia**, tali titolari dovranno inoltre assumere **un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento** che sia giuridicamente vincolante e azionabile dagli interessati (art. 40, par. 3, e art. 42, par. 2). Su come configurare un **codice di condotta** per fornire le garanzie adeguate ai fini dei trasferimenti di dati, si leggano le Linee guida dell'EDPB **[7]**. Anche sull'utilizzo della **certificazione** ai fini dei trasferimenti di dati, indicazioni utili sono contenute nelle specifiche Linee guida **[8]**.

- Il Regolamento fissa i requisiti per l'approvazione delle **norme vincolanti d'impresa** e i contenuti obbligatori di tali norme. L'elenco (art. 47, par. 2) non è esaustivo e, pertanto, ogni Autorità potrà prevedere requisiti ulteriori, a seconda dei casi. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa avviene

7 Linee guida 4/2021 sui codici di condotta come strumento per i trasferimenti - Adottate e il 22 febbraio 2022
8 "Guidelines 07/2022 on certification as a tool for transfers" - Adottate il 14 febbraio 2023

esclusivamente attraverso il meccanismo di coerenza (artt. 63-65) con l'intervento dell'EDPB (art. 64, par. 1, lett. d).

- Sono vietati trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di **decisioni giudiziarie o ordinanze amministrative emesse da Autorità del Paese terzo**, a meno dell'esistenza di accordi internazionali, in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (art. 48). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le **deroghe** previste per situazioni specifiche previste all'art. 49. A tale riguardo, si deve ricordare 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** (art. 49, par. 4) e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente. Si leggano, a tal proposito, le Linee guida EDPB sull'interpretazione delle deroghe ex art. 49 **[9]**, che forniscono criteri ai fini della corretta applicazione di questa disposizione.

9 "Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679" - Adottate il 25 maggio 2018

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Maggio 2023

STAMPA TIBURTINI srl

GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Piazza Venezia 11
00187 Roma
tel. +39 06 696771
e-mail: protocollo@gpdp.it
www.gpdp.it

Per informazioni presso l'Autorità
Ufficio relazioni con il pubblico

Orario di ricevimento telefonico
lunedì - venerdì ore 10.00 - 12.30

tel. +39 06 69677 2917

e-mail: urp@gpdp.it

Pubblicazione a cura
del Servizio relazioni esterne e media