GUIDA ALL'APPLICAZIONE DEL GDPR DELL'AUTORITA' GARANTE

Avv. Michele IASELLI

11 Luglio 2023 - dalle ore 11:30 alle 13:00

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email webinar@asmel.eu
Numero Verde 800.16.56.54 (int.3)
Web: www.asmel.eu

La 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 dilegge 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.

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.

Il GDPR 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.

Tempi dell’informativa

L’informativa deve essere fornita all’interessato prima dieffettuare 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 GDPR 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 sopraindicate.
Il Regolamento ammette inoltre l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, par. 7).

Raccomandazioni

Il GDPR 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”.

Icone


ACCESSO DATI
BASE GIURIDICA
CANCELLAZIONE
COMUNICAZIONE
CONFERIMENTO NECESSARIO
CONTITOLARI
DATI COMUNI
DATI GIUDIZIARI
DATI PARTICOLARI
DECISIONI AUTOMATIZZATE
DIFFUSIONE
DPO RDP Autore
DPO RDP EMAIL
DPO RDP TELEFONO
FINALITA'
FONTE DATI
INTERESSATO
LEGITTIMO INTERESSE
LIMITAZIONE TRATTAMENTO
MODIFICA DATI

Diritti degli interessati

Modalità per l’esercizio dei diritti

Le modalità per l’esercizio di tutti i diritti da parte degli interessatisono 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.

- Diritto di accesso
- Diritto di rettifica
- Diritto di cancellazione (e diritto all’oblio)
- Diritto di limitazione del trattamento
- Diritto di opposizione
- Diritto alla portabilità dei dati

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. 3. 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.

Approccio basato sul rischio e principio di accountability

Il GDPR 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.

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.

Adempimenti

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.

Misure di sicurezza

Le misure di sicurezza devono “garantire un livello di sicurezza adeguato al rischio” del trattamento (art. 32, par. 1).
Il GDPR 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).

Data breach

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.

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).

Trasferimento di dati verso Paesi terzi ed 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:

- *adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea (art. 45);*
- *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);*
- *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 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.
Il Regolamento consente di ricorrere anche a codici di condotta o a schemi di certificazione per dimostrare le “garanzie adeguate” previste dall’art. 46.

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.

DOMANDE