Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Regolamento (UE) n. 2016/679 adottate il 3 ottobre 2017 dal Gruppo Articolo 29 (WP 253)

Date : 5 marzo 2018

Introduzione

Il Comitato europeo per la protezione dei dati ha pubblicato a ottobre 2017 le Linee guida in materia di sanzioni amministrative previste dal Reg. 2016/679/EU.

Le sanzioni amministrative pecuniarie rappresentano un elemento centrale del nuovo regime introdotto dal Regolamento per far rispettare le norme, in quanto costituiscono una componente importante dell'insieme di strumenti di applicazione a disposizione delle Autorità di controllo, congiuntamente alle altre misure previste dall'articolo 58.

Le Linee guida sono destinate ad essere utilizzate dalle Autorità di controllo per garantire una migliore applicazione e attuazione del Regolamento ed espongono l'interpretazione comune delle disposizioni di cui all'articolo 83 del Regolamento nonché l'interazione di detto articolo con gli articoli 58 e 70 e i relativi considerando.

Le Linee guida non sono esaustive e non forniscono spiegazioni in merito alle differenze esistenti tra sistemi amministrativi, civili o penali nell'imposizione di sanzioni amministrative in generale.

Al fine di adottare un approccio coerente all'imposizione di sanzioni amministrative pecuniarie, che rispecchi adeguatamente tutti i principi delle Linee guida, il comitato europeo per la protezione dei dati ha raggiunto un'intesa comune sui criteri di valutazione di cui all'articolo 83, paragrafo 2, del Regolamento e, pertanto, il comitato e le singole Autorità di controllo concordano sull'impiego delle Linee guida come approccio comune.

Principi

Una volta accertata la violazione del Regolamento dopo aver valutato i fatti del caso, l'Autorità

di controllo competente deve individuare la o le misure correttive più appropriate per affrontare tale violazione. Le disposizioni di cui all'articolo 58, paragrafo 2, lettere da b) a j)2, indicano gli strumenti che le Autorità di controllo hanno a disposizione per far fronte a un'inadempienza da parte di un titolare del trattamento o responsabile del trattamento. Nel ricorrere a tali poteri, le Autorità di controllo devono osservare i seguenti principi:

1. La violazione del Regolamento dovrebbe comportare l'imposizione di "sanzioni equivalenti".

Sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le Autorità di controllo dei diversi Stati membri sono considerate un modo per "prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno", in linea con il considerando 13 del Regolamento.

Nei casi transfrontalieri, la coerenza deve essere garantita principalmente mediante il meccanismo di cooperazione (sportello unico) e in una certa misura tramite il meccanismo di coerenza introdotto dal nuovo Regolamento.

Nei casi nazionali previsti dal Regolamento, le Autorità di controllo applicheranno le Linee guida nello spirito di collaborazione ai sensi dell'articolo 57, paragrafo 1, lettera g), e dell'articolo 63, al fine di garantire la coerenza dell'applicazione e dell'attuazione del Regolamento. Sebbene continuino a essere indipendenti nello scegliere le misure correttive di cui all'articolo 58, paragrafo 2, le Autorità di controllo dovrebbero evitare di scegliere misure correttive differenti in casi analoghi.

Lo stesso principio si applica quando tali misure correttive sono imposte sotto forma di sanzioni pecuniarie.

2. Come tutte le misure correttive scelte dalle Autorità di controllo, le sanzioni amministrative pecuniarie dovrebbero essere "effettive, proporzionate e dissuasive".

Le Autorità di controllo dovrebbero individuare misure correttive che siano "effettive, proporzionate e dissuasive" (articolo 83, paragrafo 1), sia nei casi nazionali (articolo 55) che nei casi che comportano il trattamento transfrontaliero dei dati (secondo la definizione di cui all'articolo 4, punto 23).

Una determinazione più precisa dell'efficacia, della proporzionalità e della dissuasività scaturirà dalla pratica che emergerà in seno alle Autorità di controllo (in materia di protezione dei dati e grazie alle esperienze acquisite in altri settori normativi) e dalla giurisprudenza relativa all'interpretazione di tali principi.

Al fine di irrogare sanzioni amministrative che siano effettive, proporzionate e dissuasive, l'Autorità di controllo deve rifarsi alla definizione della nozione di impresa fornita dalla Corte di giustizia dell'Unione europea (CGUE) ai fini dell'applicazione degli articoli 101 e 102 TFUE, secondo cui il concetto di impresa va inteso come un'unità economica che può essere composta dall'impresa madre e da tutte le filiali coinvolte. Conformemente al diritto e alla

giurisprudenza dell'UE, un'impresa deve essere intesa quale unità economica che intraprende attività economiche/commerciali, a prescindere dalla persona giuridica implicata (considerando 150).

3. L'Autorità di controllo competente effettuerà una valutazione "in ogni singolo caso".

È possibile imporre sanzioni amministrative pecuniarie in risposta a una vasta serie di violazioni. Le Autorità di controllo sono incoraggiate a ricorrere alle misure correttive con un approccio ponderato ed equilibrato, al fine di reagire in maniera effettiva, dissuasiva e proporzionata alla violazione. Il punto non è qualificare le sanzioni pecuniarie come misure di ultima istanza, né evitare di irrogarle, bensì utilizzarle in un modo che non ne riduca l'efficacia come strumento. Il comitato europeo per la protezione dei dati, negli ambiti di sua competenza ai sensi dell'articolo 65 del Regolamento, adotterà una decisione vincolante sulle controversie tra le Autorità, in particolare in merito alla determinazione dell'esistenza di una violazione.

4. Un approccio armonizzato alle sanzioni amministrative pecuniarie in materia di protezione dei dati richiede la partecipazione attiva delle Autorità di controllo e lo scambio di informazioni tra le stesse.

Le Linee guida riconoscono che per alcune Autorità di controllo nazionali i poteri sanzionatori rappresentano una novità nel settore della protezione dei dati e sollevano numerose questioni in termini di risorse, organizzazione e procedura. In particolare, le decisioni in cui le Autorità di controllo esercitano i poteri sanzionatori saranno impugnabili dinanzi ai tribunali nazionali.

Criteri di valutazione di cui all'articolo 83, paragrafo 2

L'articolo 83, paragrafo 2, contiene un elenco di criteri che le Autorità di controllo devono usare per valutare sia l'opportunità di irrogare una sanzione amministrativa che l'importo della sanzione. Ciò non significa che occorre ripetere la valutazione usando gli stessi criteri, bensì che si deve procedere a una valutazione che tenga conto di tutte le circostanze di ogni singolo caso, conformemente all'articolo 83.

a) la natura, la gravità e la durata della violazione

Il Regolamento, fissando due diversi massimali per le sanzioni amministrative pecuniarie (10/20 milioni di EUR), fornisce già un'indicazione del fatto che la violazione di alcune disposizioni del Regolamento può essere più grave della violazione di altre disposizioni.

I fattori presentati di seguito devono essere valutati combinatamente, ad esempio il numero di interessati va valutato in combinazione con le possibili ripercussioni nei loro confronti.

Occorre valutare il numero di interessati coinvolti, al fine di stabilire se si tratta di un evento isolato oppure del sintomo di una violazione sistemica oppure dell'assenza di prassi adeguate. Ciò non vuol dire che gli eventi isolati non debbano essere punibili, in quanto un evento isolato potrebbe pur sempre ripercuotersi su molti interessati. A seconda delle circostanze del caso, ciò dipenderà, ad esempio, dal numero totale di soggetti registrati nella banca dati in questione, dal

numero di utenti di un servizio, dal numero di clienti, oppure dalla popolazione del paese, ove opportuno. Occorre altresì valutare la finalità del trattamento.

Se gli interessati hanno subito un danno, occorre considerarne l'entità. Il trattamento dei dati personali può generare rischi per i diritti e le libertà personali, come esposto al considerando 75:

"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati."

Anche la durata dell'infrazione può fornire un'indicazione, ad esempio, dei seguenti elementi:

- condotta intenzionale da parte del titolare del trattamento, oppure
- mancata adozione di misure preventive appropriate, oppure
- incapacità di attuare le misure tecniche e organizzative richieste.

b) il carattere doloso o colposo della violazione

In generale, il "dolo" comprende sia la consapevolezza che l'intenzionalità in relazione alle caratteristiche di un reato, mentre per "colposo" si intende che non vi era l'intenzione di causare la violazione nonostante il titolare/responsabile del trattamento abbia violato l'obbligo di diligenza previsto per legge.

Tra le circostanze indicanti il carattere doloso di una violazione figura il trattamento illecito autorizzato esplicitamente dall'alta dirigenza del titolare del trattamento oppure effettuato nonostante i pareri del responsabile della protezione dei dati o ignorando le politiche esistenti, ad esempio ottenendo e trattando dati relativi ai dipendenti di un concorrente con l'intento di screditare tale concorrente sul mercato.

Altri esempi sono: la modifica di dati personali per dare un'impressione fuorviante (positiva) circa il conseguimento degli obiettivi – episodio riscontrato nel contesto degli obiettivi relativi ai tempi d'attesa ospedalieri; lo scambio di dati personali con finalità di marketing, ossia vendita di

dati come “approvati” senza verificare/ignorando il parere degli interessati circa le modalità di utilizzo dei propri dati.

Altre circostanze, quali mancata lettura e non rispetto delle politiche esistenti, errore umano, mancata verifica dei dati personali nelle informazioni pubblicate, incapacità di apportare aggiornamenti tecnici in maniera puntuale, mancata adozione delle politiche (piuttosto che la semplice mancata applicazione) possono essere sintomo di negligenza.

Le imprese dovrebbero essere responsabili dell’adozione di strutture e risorse idonee alla natura e alla complessità della propria attività. Pertanto, i titolari del trattamento e i responsabili del trattamento non possono legittimare violazioni della normativa sulla protezione dei dati appellandosi a una carenza di risorse. Le prassi e la documentazione delle attività di trattamento seguono un approccio basato sul rischio ai sensi del Regolamento.

Esistono zone grigie che influenzano il processo decisionale circa la necessità di imporre o meno una misura correttiva e l’Autorità potrebbe dover condurre indagini più approfondite per accertare le circostanze del caso e per garantire che tutte le circostanze specifiche di ciascun caso siano state adeguatamente considerate.

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

I titolari del trattamento e i responsabili del trattamento hanno l’obbligo di attuare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, di condurre valutazioni di impatto sulla protezione dei dati e di mitigare i rischi arrecati ai diritti e alle libertà personali dal trattamento dei dati personali. Tuttavia, quando si verifica una violazione e l’interessato ne subisce i danni, la parte responsabile dovrebbe fare quanto in suo potere per ridurre le conseguenze della violazione per il o i soggetti coinvolti. Tale comportamento responsabile (o la sua assenza) sarà preso in considerazione dall’Autorità di controllo nella scelta della o delle misure correttive e nel calcolo della sanzione da imporre nel caso specifico.

Alcuni esempi potrebbero essere i seguenti:

- aver contattato altri titolari/responsabili del trattamento che potrebbero essere stati coinvolti in un’estensione del trattamento, ad esempio nel caso in cui alcuni dati sono stati erroneamente condivisi con terze parti;
- azione tempestiva adottata dal titolare/responsabile del trattamento per impedire la prosecuzione o l’espansione della violazione a un livello o a una fase che avrebbe determinato ripercussioni ben più gravi.

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

Il Regolamento ha introdotto un livello ben superiore di responsabilità del titolare del trattamento rispetto alla direttiva 95/46/CE sulla protezione dei dati.

Il grado di responsabilità del titolare del trattamento o del responsabile del trattamento valutato sulla base dell'adozione di una misura correttiva appropriata può dipendere dai seguenti aspetti:

- Il titolare del trattamento ha attuato misure tecniche che seguono i principi della protezione dei dati fin dalla progettazione o per impostazione predefinita (articolo 25)?
- Il titolare del trattamento ha attuato misure organizzative che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (articolo 25) a tutti i livelli dell'organizzazione?
- Il titolare/responsabile del trattamento ha messo in atto un livello di sicurezza adeguato (articolo 32)?
- Le prassi/politiche pertinenti in materia di protezione dei dati sono conosciute e applicate al livello adeguato di gestione dell'organizzazione? (articolo 24).

Anche se le migliori prassi dovrebbero rappresentare l'ideale da perseguire in generale, nel valutare il grado di responsabilità occorre considerare le circostanze specifiche del singolo caso.

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

Tale criterio serve per valutare i precedenti dell'entità che commette la violazione. Le Autorità di controllo dovrebbero considerare che la valutazione può avere una portata piuttosto vasta poiché ogni tipo di violazione del Regolamento, seppur di natura diversa da quella esaminata dall'Autorità di controllo, potrebbe essere pertinente ai fini della valutazione, in quanto potrebbe fornire indicazioni su un livello generale di conoscenza insufficiente o di indifferenza nei confronti delle norme sulla protezione dei dati.

L'Autorità di controllo dovrebbe valutare quanto segue:

Il titolare/responsabile del trattamento ha già commesso la stessa violazione in precedenza?

Il titolare/responsabile del trattamento ha commesso una violazione del Regolamento secondo le stesse modalità? (ad esempio a causa di una conoscenza insufficiente delle prassi esistenti nell'organizzazione, oppure in seguito a una valutazione del rischio inadeguata, non rispondendo alle richieste dell'interessato in maniera tempestiva o per un ritardo ingiustificato nel rispondere alle richieste, ecc.).

f) il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

L'articolo 83, paragrafo 2, prevede che il grado di cooperazione debba essere tenuto in "debito conto" al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa.

Un caso in cui la collaborazione con l'Autorità di controllo potrebbe essere presa in debita

considerazione è il seguente:

L’entità ha risposto in modo particolare alle richieste dell’Autorità di controllo durante la fase di indagine nel caso specifico limitando in tal modo in maniera significativa le ripercussioni sulle persone?

Detto ciò, non sarebbe opportuno tenere ulteriormente conto della collaborazione già prevista per legge: ad esempio, l’entità è in ogni caso tenuta a consentire all’Autorità di controllo di accedere ai locali per controlli/ispezioni.

g) le categorie di dati personali interessate dalla violazione;

Alcuni esempi di domande chiave a cui l’Autorità di controllo potrebbe ritenere necessario rispondere, ove opportuno, sono i seguenti:

- La violazione riguarda il trattamento di categorie particolari di dati di cui agli articoli 9 e 10 del Regolamento?
- I dati sono direttamente/indirettamente identificabili?
- Il trattamento riguarda dati la cui diffusione causerebbe immediati danni/disagi alla persona (che non rientrano nelle categorie di cui agli articoli 9 e 10)?
- I dati sono direttamente disponibili senza protezioni tecniche oppure sono criptati?

h) la maniera in cui l’Autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

L’Autorità di controllo potrebbe venire a conoscenza della violazione in seguito a indagini, reclami, articoli di giornale, suggerimenti anonimi oppure notifiche da parte del titolare del trattamento. Il titolare del trattamento ha l’obbligo a norma del Regolamento di notificare all’Autorità di controllo eventuali violazioni dei dati personali. Qualora il titolare del trattamento si limiti ad adempiere a tale obbligo, la conformità ad esso non può essere interpretata come fattore attenuante/mitigante. Analogamente, qualora il titolare/responsabile del trattamento abbia agito incautamente senza notificare la violazione, o perlomeno senza notificarne tutti i dettagli, in quanto non in grado di valutarne adeguatamente la portata, l’Autorità di controllo potrebbe ritenere necessaria l’imposizione di una sanzione più grave, il che significa che risulterà improbabile la classificazione quale violazione minore.

i) il rispetto di precedenti provvedimenti dell’autorità di controllo relativamente allo stesso oggetto;

Il titolare del trattamento o il responsabile del trattamento potrebbe già essere nel mirino dell’Autorità di controllo per la verifica della conformità in seguito a una precedente violazione. In tal caso gli eventuali precedenti contatti con il responsabile della protezione dei dati saranno stati verosimilmente numerosi e l’Autorità di controllo li terrà in considerazione.

j) l’adesione ai codici di condotta approvati ai sensi dell’articolo 40 o ai meccanismi di

certificazione approvati ai sensi dell’articolo 42;

Qualora il titolare del trattamento o il responsabile del trattamento abbia aderito a un codice di condotta approvato, l’Autorità di controllo potrebbe ritenere sufficiente che la comunità incaricata di gestire il codice intervenga adeguatamente in prima persona nei confronti del proprio membro, ad esempio tramite i regimi di monitoraggio e applicazione del codice di condotta stesso. Pertanto, l’Autorità di controllo potrebbe ritenere che tali misure siano sufficientemente effettive, proporzionate e dissuasive in quel particolare caso senza che l’Autorità di controllo stessa debba imporre misure aggiuntive. Alcune forme di sanzionamento dei comportamenti non conformi possono avvenire tramite il regime di monitoraggio, ai sensi dell’articolo 41, paragrafo 2, lettera c), e dell’articolo 42, paragrafo 4), compresa la sospensione o l’esclusione del titolare del trattamento o del responsabile del trattamento dalla comunità incaricata di gestire il codice. Ciononostante, i poteri dell’organismo di controllo si espletano “fatti salvi i compiti e i poteri dell’Autorità di controllo competente”, il che significa che l’Autorità di controllo non ha l’obbligo di tenere conto delle sanzioni precedentemente imposte relative al regime di autoregolamentazione.

La non conformità con le misure di autoregolamentazione potrebbe altresì rivelare la colpa o il dolo del titolare/responsabile del trattamento.

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Le informazioni relative ai profitti derivanti da una violazione potrebbero risultare particolarmente importanti per le Autorità di controllo in quanto il guadagno economico derivante dalla violazione non può essere compensato tramite misure che non abbiano una componente pecuniaria. Pertanto, il fatto che il titolare del trattamento abbia tratto profitto dalla violazione del Regolamento può costituire una chiara indicazione della necessità di imporre una sanzione pecuniaria.

Conclusioni

In sintesi, le Autorità devono ripristinare la conformità tramite tutte le misure correttive che hanno a disposizione. Le Autorità di controllo dovranno altresì scegliere il canale più appropriato per portare avanti l’intervento (potendo ricorrere, ad esempio, a sanzioni penali - ove disponibili a livello nazionale).

La pratica di applicare sanzioni amministrative pecuniarie coerentemente all’interno dell’Unione europea è una pratica in via di evoluzione. Le Autorità di controllo dovrebbero collaborare costantemente per aumentare tale coerenza, ad esempio tramite regolari scambi durante seminari sul trattamento dei casi o altri eventi che consentano di confrontare i casi a livello sub-nazionale, nazionale e transfrontaliero.

A cura di: **Elena Bassoli**