CONSULENTI DI DIREZIONE ASSOCIATI

GDPR: sanzioni pecuniarie fisse e proporzionali al fatturato

Il GDPR ridisegna l'impianto sanzionatorio in tema di privacy. Un elemento centrale del nuovo assetto è rappresentato dalle sanzioni amministrative pecuniarie. Una volta accertata la violazione di una o più norme del GDPR, l'autorità di controllo competente individua le misure correttive più appropriate. Le sanzioni applicate devono essere equivalenti in tutti gli Stati membri e rispondere adeguatamente alla natura, alla gravità e alle conseguenze della violazione. L'aspetto più preoccupante è quello relativo alle sanzioni d'importo non fisso, ma commisurato al fatturato globale annuo della società.

Quali le possibili conseguenze per le imprese?

L'Unione Europea, con il GDPR, ha voluto attuare una riforma completa del quadro normativo sulla protezione dei dati.

Una simile riforma si è dovuta fondare su alcuni principi fondamentali: norme specifiche e coerenti, procedure consultive e di accertamento semplificate, azioni coordinate anche tra i vari Paesi, utenti messi al centro del sistema di protezione, informazioni sui diritti più efficaci e rafforzamento dei poteri indirizzati a far rispettare le norme previste.

Le sanzioni amministrative pecuniarie rappresentano, in particolare, un elemento centrale di questo nuovo regime, in quanto rientrano nell'insieme degli strumenti di applicazione che sono messi a disposizione della autorità di controllo in ogni singolo Paese.

Una volta accertata la violazione di alcune norme del GDPR, l'autorità di controllo competente può individuare le misure correttive più appropriate per affrontare la situazione che si è così venuta a creare. Le disposizioni di cui all'Articolo 58, Paragrafo 2, indicano gli strumenti messi a disposizione per far fronte a un'inadempienza da parte di un titolare o di un responsabile del trattamento.

Sanzioni equivalenti in tutti gli Stai membri

Innanzitutto, la violazione del GDPR dovrebbe comportare l'imposizione di "sanzioni equivalenti". Infatti, al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione Europea, il livello di protezione dovrebbe essere equivalente in tutti gli Stati membri. Per garantire questo, occorrono – tra l'altro – poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali, nonché sanzioni equivalenti in caso di violazione.

Il Regolamento offre una base più solida rispetto alla Direttiva 95/46/CE, in quanto lo stesso è direttamente applicabile negli Stati membri, ed esorta a una maggiore coerenza, da garantire principalmente mediante il meccanismo di cooperazione.

Sanzioni pecuniarie proporzionate e dissuasive

Come tutte le misure correttive, le sanzioni amministrative pecuniarie dovrebbero rispondere adeguatamente alla natura, alla gravità e alle conseguenze della violazione. Le autorità di controllo dovranno allora valutare tutte le circostanze del caso in maniera coerente e

oggettivamente giustificata: la valutazione di quanto le misure siano effettive, proporzionate e dissuasive in ciascun caso dovrà riflettere anche l'obiettivo che esse perseguono, che potrà essere quello di ripristinare la conformità alle norme o quello di punire un comportamento illecito. Il Regolamento, fissando due diversi massimali per le sanzioni amministrative pecuniarie (10 e 20 milioni di euro), fornisce già un'indicazione sul fatto che la violazione di alcune disposizioni del Regolamento si può presentare più grave rispetto alla violazione di altre.

Nel caso in cui l'autorità di controllo ritenga che la violazione non crei un rischio significativo per i diritti degli interessati e non incida sull'essenza dell'obbligo in questione, la sanzione può talvolta essere sostituita da un ammonimento. Tale sostituzione può avvenire anche nel caso in cui il titolare del trattamento sia una persona fisica e la sanzione pecuniaria che dovrebbe essere imposta costituisca un onere sproporzionato per la "vittima" di tale provvedimento.

Come si determina la gravità della violazione

La natura della violazione, l'oggetto o la finalità del trattamento in questione, nonché il numero di interessati lesi dal danno e il livello del danno da essi subito, possono fornire chiaramente un'indicazione della gravità della violazione.

Occorre valutare, in particolare, il numero di interessati coinvolti al fine di stabilire se si tratti di un evento isolato oppure un sintomo di una violazione sistematica o, addirittura, dell'assenza volontaria e perdurante di prassi adeguate alla protezione dei dati in quel contesto specifico.

Se, poi, gli interessati hanno subito un danno, occorre considerarne l'entità.

Un'ulteriore distinzione che deve essere operata è quella tra violazione colposa e violazione dolosa: quest'ultima è generalmente riconosciuta come più grave e, dunque, potrebbe essere idonea a giustificare l'applicazione di una sanzione amministrativa pecuniaria.

Tra le circostanze indicanti il carattere doloso di una violazione potrebbe figurare il trattamento illecito autorizzato esplicitamente dall'alta dirigenza del titolare, oppure effettuato ignorando le politiche esistenti. Altre circostanze, invece, come l'errore umano o l'incapacità di apportare aggiornamenti tecnici in maniera puntuale, potrebbero essere sinonimo di negligenza.

Non possono essere legittimate violazioni della normativa, e questo risulta chiaro nel Regolamento, facendo appello a una carenza di risorse economiche o di personale. I titolari del trattamento e i responsabili del trattamento, infatti, hanno l'obbligo di attuare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, di condurre valutazioni d'impatto sulla protezione dei dati e di mitigare i rischi arrecati ai diritti e alle libertà personali.

Quando si verifica una violazione e ne derivano danni, la parte responsabile dovrebbe fare quanto in suo potere per ridurre le conseguenze negative: tale comportamento responsabile (o la sua assenza) sarà preso in considerazione dall'autorità di controllo nella scelta della misura correttiva e della sanzione da imporre.

In passato, l'esperienza disciplinare delle autorità di controllo nell'ambito della Direttiva 95/46/CE ha dimostrato che può essere opportuno mostrare un certo livello di flessibilità nei confronti di quei titolari/responsabili del trattamento che hanno ammesso la violazione e che si sono assunti la responsabilità di correggere o limitare l'impatto delle loro azioni.

Aumenta il grado di responsabilità del titolare del trattamento

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 suo grado di responsabilità, valutato sulla base dell'adozione di una misura correttiva appropriata, può dipendere dai seguenti aspetti:
se sono state attuate misure tecniche che seguono i principi della protezione dei dati fin dalla progettazione o per impostazione predefinita;
se sono state adottate misure organizzative che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita a tutti i livelli dell'organizzazione;
se è stato messo in atto un livello di sicurezza adeguato;
se le prassi/politiche pertinenti in materia di protezione dei dati sono conosciute e applicate al livello adeguato di gestione dell'organizzazione.
L'Articolo 25 e l'Articolo 32 del Regolamento UE (GDPR) prevedono che i titolari del trattamento tengano conto "della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche". Anziché imporre un obbligo di risultato, tali disposizioni introducono obblighi di mezzi, il che significa che il titolare del trattamento deve condurre le valutazioni necessarie e giungere alle opportune conclusioni.

L'autorità di controllo, inoltre, dovrebbe valutare eventuali precedenti violazioni pertinenti commesse dal titolare o dal responsabile del trattamento, osservando in particolare se si è trattato della medesima violazione o di una violazione eseguita con le stesse modalità.

E se le violazioni sono molteplici?

È possibile comminare sanzioni amministrative pecuniarie in risposta ad una vasta serie di violazioni.

Il Regolamento stabilisce che ogni caso sia valutato singolarmente: pertanto, al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singola fattispecie, si deve tenere conto di una serie di elementi espressamente elencati dalla disposizione in esame. A seguito di tale valutazione, l'autorità di controllo ha la responsabilità di scegliere la misura più adeguata, nonché il canale più appropriato per portare avanti l'intervento.

Controversie e rapporti tra le autorità

In caso di controversie tra le autorità, in particolare in merito alla determinazione dell'esistenza di una violazione, sarà il Comitato Europeo per la Protezione dei dati ad adottare una decisione vincolante, esaminando anche se, e in che modo, la misura correttiva adottata nel singolo caso rispetti i principi di efficacia, proporzionalità e deterrenza richiesti dal regolamento.

Un approccio armonizzato richiede altresì la partecipazione attiva delle autorità di controllo e lo scambio d'informazioni tra le stesse. 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.

Ad ogni modo, le diverse autorità dovrebbero collaborare tra loro e, ove necessario, con la Commissione europea, al fine di sostenere scambi formali e informali di informazioni. Tale cooperazione si concentrerà sulla loro esperienza e pratica nell'applicazione di poteri sanzionatori, con l'obiettivo di raggiungere una maggiore coerenza complessiva dell'intero sistema.

Sanzioni proporzionali al fatturato

La parte che più preoccupa, con riferimento alle sanzioni, è quella che prevede sanzioni non d'importo/massimale fisso ma commisurate al fatturato globale annuo della società.

L'idea di prevedere sanzioni in percentuale al fatturato è nata per cercare di "intimorire" anche le grandi società o piattaforme nordamericane (ma non solo) e intaccare direttamente il loro business, cosa che con sanzioni fisse, seppur alte, non sarebbe stato possibile fare. Al contempo, simili sanzioni, che l'autorità di controllo può riferire al fatturato mondiale (o della casa madre che dir si voglia), sono pensate per responsabilizzare anche le business unit e sedi operative locali di grandi multinazionali con sede centrale al di fuori dell'Italia. Una violazione del GDPR perpetrata da una di queste sedi, anche se piccola, inciderà infatti, in punto di sanzioni, sul bilancio di tutta la società.