CONSULENTI DI DIREZIONE ASSOCIATI

Privacy, PMI: le strategie per evitare le sanzioni

Il GDPR prevede per le PMI sanzioni di importo variabile, e talvolta elevato, a seconda della violazione commessa relativamente al trattamento dei dati. Diventa, quindi, fondamentale per le piccole e medie imprese comprendere non solo come evitare le sanzioni, ma anche come far sì che determinati comportamenti possano mitigarne l'entità o addirittura annullarle. In particolare, per le violazioni dei diritti dell'interessato, dei principi del trattamento e delle norme sul trasferimento dei dati all'estero sono previste sanzioni fino a 20 milioni di euro e al 4% del fatturato globale annuo mondiale dell'azienda. È possibile effettuare un'analisi della probabilità di incorrere in sanzioni?

Il GDPR prevede un quadro sanzionatorio molto articolato per le PMI che, da un lato, cerca di includere ogni possibile violazione e, dall'altro, cerca di fornire all'autorità di controllo (Garante) la possibilità di graduare la sanzione a seconda di alcuni parametri particolarmente interessanti.

Gradualità delle sanzioni

Non ci si riferirà, infatti, soltanto della gravità concreta del fatto, ma anche alla dimensione dell'azienda, al danno effettivamente arrecato ai soggetti e alla buona condotta dell'azienda prima e dopo, ossia in base a quale impegno era stato dimostrato prima ai fini degli adempimenti obbligatori e a quale impegno viene dimostrato dopo per cercare di rimediare ai fatti/incidenti avvenuti e per limitare l'esposizione al danno dei diritti degli utenti.

Le sanzioni previste sono, per una PMI, molto alte. Ciò significa che diventa fondamentale comprendere non solo come evitarle ma anche come far sì che determinati comportamenti possano, in caso di sanzione, mitigarne l'entità o addirittura annullarla.

L'articolo 84 del GDPR prevede, innanzitutto, che la materia penale sarà disciplinata da ogni singolo Stato, quindi le sanzioni hanno natura amministrativa. Ciò non toglie, si diceva, che possano essere particolarmente pesanti per una piccola realtà.

Criteri per l'applicazione delle sanzioni

In linea di principio, le sanzioni pecuniarie amministrative dovranno essere armonizzate tra i vari Stati e dovranno osservare criteri di effettività, proporzionalità e dissuasività.

L'articolo 83 del GDPR è chiaro nel disporre che le sanzioni debbano essere applicate in funzione del singolo caso e tenendo conto della natura, della gravità e della durata della violazione, delle finalità del trattamento, del numero di interessati lesi e del livello del danno, oltre al carattere colposo o doloso della violazione.

Sono previste due macro-categorie di violazioni, una prima più lieve, che coinvolge ad esempio i nuovi adempimenti in materia di misure di sicurezza, fino a 10 milioni di euro o al 2% del fatturato globale annuo mondiale dell'azienda, e una seconda collegata alle violazioni dei diritti dell'interessato, dei principi del trattamento, delle norme sul trasferimento dei dati all'estero, con sanzioni fino a 20 milioni di euro e al 4% del fatturato.

È probabile che la norma italiana che disciplinerà, nei prossimi mesi, la transizione dal "vecchio" Codice Privacy al nuovo quadro, indicherà con più precisione gli importi per le PMI, e che a livello europeo si penserà a sanzioni equivalenti in tutti gli Stati membri.

In caso di eventi irrisori e che non presentano rischi significativi per gli interessati, ci potrà essere una diffida in alternativa alla sanzione pecuniaria, e interessante sarà anche valutare il grado di cooperazione fornito dalla PMI per creare un quadro di sanzioni che sarà graduale.

È necessario prestare attenzione in un'ottica di sanzioni alla violazione dei dati personali che il GDPR definisce chiaramente come una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Violazione dei dati e gravità delle sanzioni

In un'ottica di gravità di sanzioni, i dati più delicati sono di tre tipi:

i) genetici;

ii) biometrici;

iii) relativi alla salute.

In altre parole, la PMI che tratta dati simili deve essere consapevole che le sanzioni più gravi sono spesso correlate alla diffusione illecita di simili dati.

I primi, i dati genetici, sono quei dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona, e che risultano in particolare dall'analisi di un campione biologico dell'individuo. Oggi i dati genetici sono diventati molto comuni e non sono più trattati soltanto in ospedali, cliniche o laboratori ma anche con kit domestici poco costosi.

I secondi, i dati biometrici, sono quei dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici. Al GDPR e al Garante interessano in quanto sono processabili elettronicamente, ossia la fotografia di un viso, ad esempio, può essere analizzata e utilizzata da un software.

I terzi sono invece quei dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Ridurre il rischio di sanzioni

Importante è, soprattutto nelle piccole realtà, analizzare la probabilità delle sanzioni e valutare, con riferimento all'orientamento sanzionatorio del Garante nei vent'anni precedenti al GDPR, quali sono stati gli ambiti dove sono intervenute delle criticità.

Sicuramente, l'attenzione all'informativa, sia se omessa, sia se incompleta, e il trattamento illecito dei dati, insieme alle misure di sicurezza, sono i tre ambiti dove le sanzioni potranno "cadere".

Un buon modo di procedere, a fini predittivi, è quello di individuare i principi di base che il GDPR stabilisce con riferimento ai trattamenti, e individuare quindi se i trattamenti siano effettuati in violazione di legge (ossia in maniera illecita).

In particolare, i dati personali dovrebbero essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ("limitazione della finalità");

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

L'attività di previsione delle sanzioni, anche nella piccola e media impresa, dovrà essere condotta partendo da tali principi.

Di particolare interesse sono i punti che riguardano i tempi di conservazione (molte sanzioni hanno colpito società che custodivano dati in eterno o oltre i limiti previsti per legge), il fatto che i dati debbano essere trattati sempre e comunque per le finalità per le quali sono stati raccolti e la necessità di approntare misure di sicurezza adeguate.