BIBLIOTECA

GDPR: protezione dai rischi, liceità e sanzioni

Introduzione

In questo video vediamo insieme:

- come proteggersi dai possibili rischi per il trattamento dei dati personali
- quali sono le condizioni di liceità di utilizzo dei dati secondo il GDPR
- quali sono le eventuali sanzioni in cui si può incorrere

I possibili rischi

Il trattamento di dati può comportare rischi, più o meno elevati, che possono ledere i diritti e le libertà delle persone fisiche e che possono cagionare danni materiali o immateriali.

I possibili rischi riguardano:

- la distruzione
- la modifica
- l'accesso accidentale o illegale
- la divulgazione non autorizzata dei dati personali trasmessi

Danni immateriali e materiali

A causa di questi rischi, come dicevamo, le persone possono subire danni immateriali e materiali.

Per danni immateriali intendiamo:

- la perdita di controllo sui dati
- la limitazione dei diritti dell'Interessato
- una discriminazione dell'Interessato
- il rischio di un danno reputazionale

I rischi materiali prevedono:

1. la violazione delle misure della sicurezza
2. perdite finanziarie
3. perdite di quote di mercato a favore di concorrenti
4. altri rischi di tipo economico

Esempi di trattamenti a rischio elevato

Il GDPR indica nell'art.35 alcuni esempi di trattamenti che possono comportare un rischio elevato:

- quando il trattamento consiste in una valutazione sistematica e globale di aspetti personali relativi a persone fisiche attraverso un procedimento automatizzato e che possono avere effetti giuridici o comunque significativi sulle persone fisiche stesse
- quando viene effettuato un trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati
- quando si effettua una sorveglianza sistematica su larga scala di una zona accessibile al pubblico

Approccio “risk-based”

Per prevenire, evitare e minimizzare i rischi, il GDPR ha introdotto un nuovo approccio metodologico definito “risk-based”.

Questo approccio è basato sulla protezione dei dati dell'utente e sulla valutazione dell'effettivo rischio per ogni società.

La valutazione del rischio (risk assessment) è un insieme di attività volte a identificare i rischi, calcolarne il livello e decidere se sono accettabili o da mitigare.

Misure tecniche e organizzative adeguate

Il GDPR prevede quindi che il Titolare e il Responsabile del trattamento mettano in atto misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio.

In questo devono tenere conto:

- dello stato dell'arte
- dei costi di attuazione
- della natura, dell'ambito, del contesto, delle finalità e dei rischi del trattamento

Diventa quindi necessario capire quali siano le misure adeguate che la situazione concreta richiede di adottare.

Ad esempio le misure tecniche possono essere:

- la pseudonimizzazione
- la cifratura
- l'inserimento della privacy nei processi e nell'organizzazione aziendale già nella fase di progettazione (privacy by design)
- la protezione per impostazione predefinita che comporti il trattamento solo dei dati strettamente necessari (privacy by default)
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali
- il ripristino tempestivo dei dati e dell'accessibilità in caso di incidente fisico o tecnico

Le misure organizzative invece possono riguardare:

- la designazione di responsabili del trattamento e referenti interni
- la nomina di un DPO

- la creazione di policy, di disciplinari e di linee guida
- l'esecuzione di corsi di formazione per istruire i soggetti interessati
- l'esistenza di procedure interne

Criteri di valutazione

Questi sono solo alcuni esempi.

Caso per caso deve essere effettuata una valutazione, scegliendo le misure adatte:

- alla tipologia di trattamento
- alle finalità perseguite
- alla natura dei dati trattati
- ai diritti e libertà in gioco

Le misure devono tenere in considerazione anche i rischi e i costi che la loro implementazione comporta.

Periodicamente devono inoltre essere verificate e valutate per assicurarne l'efficacia nel tempo.

Condizioni di liceità

Una volta ottemperate tutte le misure organizzative e di sicurezza, i dati possono essere trattati secondo le condizioni di liceità sancite dal GDPR.

Affinché il trattamento dei dati sia lecito deve ricorrere almeno una delle seguenti condizioni:

- l'Interessato ha prestato il proprio consenso
- il trattamento è strettamente necessario all'esecuzione di un contratto o di misure pre-contrattuali di cui l'Interessato è parte
- il trattamento è necessario per adempiere a un obbligo legale di cui è soggetto il Titolare
- serve per salvaguardare interessi vitali dell'Interessato
- è necessario per l'esecuzione di compiti di interesse pubblico
- persegue un legittimo interesse del Titolare del trattamento a condizione che tale interesse legittimo sia perfettamente bilanciato con la libertà e i diritti dell'Interessato

Sanzioni amministrative

Qualora non vengano ottemperati gli obblighi sanciti dal GDPR si può incorrere in sanzioni amministrative e in sanzioni penali.

Le sanzioni amministrative più alte arrivano fino a 20 milioni di euro o al 4% del fatturato globale annuo e si applicano a

- violazioni dei principi del trattamento, incluse le condizioni per il consenso
- violazioni dei diritti degli Interessati
- inosservanza delle norme in tema di trasferimento internazionale dei dati

Le sanzioni amministrative più basse arrivano fino a 10 milioni di euro o al 2% del fatturato globale annuo e si applicano alla violazione delle obbligazioni di Titolari e Responsabili.

Il Garante

L'organo competente a irrorare le sanzioni è il Garante che dovrà tenere presenti:

- la natura, la gravità e la durata della violazione
- il carattere doloso o colposo della violazione
- le categorie di dati personali interessate dalla violazione
- eventuali precedenti violazioni commesse

Sanzioni penali

Le sanzioni penali decretate dal legislatore italiano riguardano:

- il trattamento illecito di dati personali
- l'acquisizione fraudolenta, la comunicazione e la diffusione illecita di dati personali oggetto di trattamento su larga scala
- le false dichiarazioni rese al Garante
- l'inosservanza dei provvedimenti del Garante