Regolamento generale sulla protezione dei dati

Il Regolamento generale sulla protezione dei dati (GDPR) è un regolamento dell'Unione europea (Ue) che stabilisce un nuovo accordo quadro relativo alla gestione e protezione dei dati personali per i cittadini europei.

Esso introduce nuovi obblighi e responsabilità per tutte le organizzazioni che gestiscono dati personali, nonché nuovi diritti che regolano le modalità con cui i dati dati delle persone vengono raccolti, elaborati e archiviati.

Effetti del GDPR

Se la tua organizzazione deve essere conforme al GDPR, è necessario prendere in considerazione una serie di fattori. Consigliamo vivamente di richiedere una consulenza legale per determinare che cosa potrebbe essere necessario per la tua situazione specifica.

1. Comprendere i propri dati

Proteggere i dati in maniera adeguata significa comprendere come vengono trattati all'interno della tua organizzazione, ovvero il modo in cui i dati personali vengono gestiti, condivisi, utilizzati, archiviati ed eliminati. Comprendere che cosa siano i dati e come vengono utilizzati e conservati è un requisito fondamentale per la creazione della strategia GDPR della tua azienda.

2. Determinare la proprietà e la responsabilità

È importante identificare un proprietario responsabile per la conformità della protezione dei dati. Per alcune organizzazioni è obbligatorio designare un responsabile della protezione dei dati.Il GDPR ha inoltre introdotto un nuovo principio di "responsabilità" che impone alle organizzazioni di adottare un programma di conformità alla protezione dei dati. Le organizzazioni dovranno sviluppare delle politiche interne di tutela dei dati e fornire una formazione specifica al personale.

3. Garantire una base giuridica per il trattamento

Un altro elemento del GDPR che le aziende devono garantire che sia documentato sono le basi giuridiche per il trattamento dei diversi tipi di dati personali che si gestiscono. Ad esempio, se si utilizza il consenso come base per il trattamento, si dovrà considerare come ottenerlo ed essere in grado di dimostrare chiaramente come e quando è stato fornito.

4. Comprendere i diritti dei soggetti interessati

Per garantire che le procedure siano adeguate, è necessario assicurarsi di comprendere i diritti delle persone in relazione ai propri dati personali. Ad esempio, i soggetti interessati hanno il diritto di accedere ai propri dati personali, nonché di correggerli, eliminarli o esportarli in via elettronica. In determinate circostanze, gli utenti hanno il diritto di opporsi al processo decisionale e alla profilazione automatizzati.

5. Garantire il principio privacy by design

Con "privacy by design" (privacy incorporata nella progettazione) si intende un requisito legale esplicito presente fin dall'inizio di un progetto, perciò è importante pensare bene a come integrarlo nei processi aziendali. In alcune circostanze, è necessario anche condurre valutazioni dell'impatto sulla privacy.

6. Preparazione alla gestione delle violazioni

Per un solido programma di protezione dei dati, è fondamentale garantire che le politiche e i processi di gestione delle violazioni dei dati siano aggiornati e soggetti a test. Il GDPR impone l'individuazione e la tempestiva segnalazione di violazioni alle autorità competenti. Eventuali violazioni o una mancata segnalazione di esse possono comportare delle multe.

7. Comunicare le informazioni essenziali

Garantire che le politiche sulla privacy online e altre comunicazioni della propria organizzazione siano aggiornate e comprendano le pratiche di tutela dei dati. Secondo i nuovi requisiti, è necessario fornire una descrizione dettagliata della base giuridica del trattamento e informare gli utenti riguardo all'autorità presso la quale possono presentare un reclamo in caso di problemi.

8. Lavorare con i fornitori

L'adempimento agli obblighi del GDPR va oltre le politiche della tua organizzazione. Eventuali terze parti che trattano dati personali per tuo conto dovranno soddisfare gli standard necessari per la protezione dei dati. Alcune domande che potresti voler porre ai tuoi provider:

- Disponete di solide pratiche per la sicurezza di rete e delle informazioni, per la privacy e per la protezione dei dati?
- Siete conformi agli standard accettati a livello internazionale? È possibile verificare la vostra conformità?
- Come potete dimostrare una forte cultura improntata sulla fiducia e sulla sicurezza? E quali controlli offrite per aiutare le aziende a gestire i dati e a rispettare gli obblighi in qualità di responsabili del trattamento?

Dropbox: proteggiamo i tuoi dati

La fiducia è alla base del nostro rapporto con milioni di persone e aziende in tutto il mondo.

La fiducia che hai riposto in noi è molto importante e ci assumiamo la responsabilità di proteggere le tue informazioni con la massima serietà. Per guadagnarci la tua fiducia, abbiamo creato Dropbox e continueremo a migliorarlo prestando particolare attenzione a sicurezza, conformità e privacy.

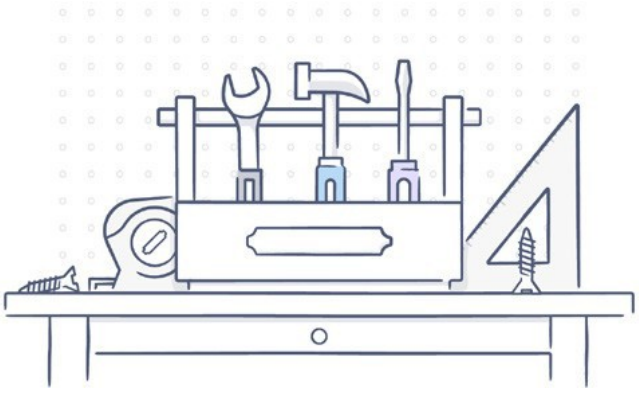
Sicurezza: protezione e controllo

Proteggi: la sicurezza dell'architettura e delle informazioni

Dropbox è progettato con un'infrastruttura sicura, distribuita su parecchi livelli di protezione, che include trasferimento dati, crittografia, configurazione della rete e controlli a livello di applicazione distribuiti in un'infrastruttura scalabile e affidabile. Il nostro solido accordo quadro per la gestione della sicurezza è progettato per valutare i rischi e creare una cultura della sicurezza in Dropbox. Revisioniamo e aggiorniamo regolarmente le politiche di sicurezza; offriamo ai nostri dipendenti una formazione sulla sicurezza; eseguiamo test di sicurezza delle applicazioni e della rete (compresi test di vulnerabilità); eseguiamo la valutazione dei rischi e monitoriamo la conformità con le politiche di sicurezza. Tutti i dettagli sono disponibili nel nostro White Paper sulla sicurezza di Dropbox Business.

Controllo: potenziare gli amministratori IT

Dropbox fornisce le funzioni di visibilità e controllo di cui hanno bisogno gli amministratori IT per agevolarti nella gestione dei tuoi obblighi di conformità. La nostra dashboard amministratore ti consente di monitorare l'attività del tuo team, vedere i dispositivi collegati e ottenere un rapporto sull'attività di condivisione.
È possibile creare gruppi per gestire facilmente l'accesso dei membri del team a cartelle specifiche; la gestione delle cartelle del team ti offre visibilità e controllo su tutte le attività che le riguardano, comprese le opzioni di sincronizzazione. Con le autorizzazioni di accesso ai link puoi creare password per proteggere i link condivisi, impostare date di scadenza per consentire accessi temporanei e limitare l'accesso solo ai membri della tua organizzazione. Il nostro strumento di trasferimento dell'account ti consente di trasferire facilmente i file da un utente all'altro quando cambiano le responsabilità. Elimina in remoto i tuoi file da dispositivi rubati o perduti



Compliance: fiducia e verifica

La conformità rappresenta un modo efficace per verificare l'affidabilità di un servizio. Ti invitiamo a verificare che le nostre pratiche di sicurezza siano conformi agli standard e alle normative più diffusi, come ISO 27001, 27017, 27018 e SOC 1, 2 e 3. I nostri revisori di terze parti indipendenti mettono alla prova i controlli da noi effettuati e forniscono report e opinioni, che condividiamo con te quando possibile. Ulteriori informazioni sugli standard ai quali siamo conformi e sul modo in cui testiamo le nostre pratiche di sicurezza sono disponibili sulla nostra pagina complianceweb.

Privacy: il nostro impegno

I tuoi dati, sia personali che di lavoro, sono di tua proprietà e ci impegniamo a garantirne la riservatezza. La nostra politica sulla privacy descrive chiaramente come gestiamo e tuteliamo le tue informazioni. Pubblichiamo un rapporto di trasparenza e i principi relativi alle richieste ufficiali di dati per condividere informazioni sulla frequenza con cui riceviamo, analizziamo e rispondiamo a tali richieste; inoltre, cerchiamo di riformare le leggi per aumentare il livello di tutela della tua privacy.

Lavorare insieme per proteggere i dati

Dropbox collabora con i suoi clienti aziendali per mantenere i loro dati al sicuro. Adottiamo misure globali per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni; formiamo i nostri dipendenti sulle pratiche di sicurezza e privacy; creiamo una cultura in cui l'affidabilità è la massima priorità; e sottoponiamo i nostri sistemi e pratiche a rigorosi test e valutazioni di terze parti. Anche i clienti giocano un ruolo fondamentale nel garantire che i team e i dati siano protetti e al sicuro. Dropbox ti consente di configurare, utilizzare e monitorare il tuo account in modi che rispettano le esigenze di sicurezza, privacy e conformità della tua organizzazione. La nostra guida alla responsabilità condivisa può aiutarti a capire di più su ciò che facciamo per mantenere il tuo account al sicuro e su ciò che puoi fare per mantenere visibilità e controllo sui dati del tuo team.