Règlement général sur la protection des données

Le Règlement général sur la protection des données, ou RGPD, est une réglementation de l'Union européenne qui définit un nouveau cadre juridique pour le traitement et la protection des données personnelles des citoyens de l'Union européenne.

Elle introduit de nouvelles obligations et responsabilités pour toutes les entreprises qui traitent des données personnelles, et de nouveaux droits pour les individus concernant la façon dont leurs données sont collectées, traitées et stockées.

Les conséquences du RGPD

Si votre entreprise doit se conformer au RGPD, vous devez prendre en compte un certain nombre de facteurs. Nous vous recommandons de faire appel à un conseiller juridique pour connaître les spécificités liées à votre situation.

1. Comprendre vos données

Pour protéger les données de façon appropriée, vous devez comprendre comment votre entreprise les traite, c'est-à-dire comment les données personnelles sont gérées, partagées, utilisées, archivées et supprimées. Comprendre la nature des données, ainsi que la façon dont elles sont utilisées et stockées, est un élément clé de votre stratégie RGPD.

2. Déterminer la propriété et la responsabilité

Identifier un responsable de mise en conformité est essentiel. Dans certaines entreprises, nommer un délégué à la protection des données est obligatoire. Le RGPD a aussi instauré un nouveau principe de responsabilité qui exige des entreprises qu'elles adoptent un programme de conformité pour la protection des données. Dans ce cadre, elles doivent mettre au point des politiques de protection des données et former leurs employés.

3. Définir une base juridique pour le traitement des données

Dans le cadre du RGPD, les entreprises doivent également s'assurer de documenter les motifs d'ordre juridique justifiant le traitement des différents types de données personnelles. Par exemple, si la façon dont vous traitez les données repose sur le consentement des utilisateurs, vous devrez réfléchir à la façon de l'obtenir et devez être capable de démontrer clairement à quel moment et de quelle façon vous l'avez obtenu.

4. Comprendre les droits des utilisateurs

Pour vous assurer que les procédures que vous mettez en place conviennent à vos utilisateurs, vous devez comprendre leurs droits en matière de données personnelles. Par exemple, les utilisateurs ont le droit d'accéder à leurs données personnelles, ainsi que de demander à les modifier, supprimer ou exporter électroniquement. Dans certains cas, ils ont également le droit de s'opposer au profilage et aux prises de décisions automatisées.

5. Garantir la protection des données dès la conception

La protection des données dès la conception constituant pour la première fois une obligation juridique, il est important de l'intégrer à vos processus. Dans certains cas, vous devrez également réaliser une évaluation de l'impact de la protection des données.

6. Se préparer aux risques de violation des données

Vous devez vous assurer que vos stratégies et processus de gestion des violations de données sont à jour et testés. Ce point est essentiel pour bénéficier d'un programme de protection des données efficace. La détection et le signalement rapides des violations des données aux autorités compétentes sont des obligations du RGPD. Vous serez visé par une amende si vous ne signalez pas les défaillances et violations.

7. Communiquer les informations principales

Vous devez vous assurer que la politique de confidentialité en ligne ainsi que les autres notifications de votre entreprise sont à jour et couvrent les pratiques de protection des données. Selon les nouvelles obligations, vous devez détailler la base juridique régissant le traitement des données et vous devez informer les utilisateurs des autorités auprès desquelles ils peuvent déposer une plainte en cas de problème.

8. Travailler avec vos fournisseurs

La conformité au RGPD va bien au-delà de vos propres politiques de sécurité. Tous les tiers qui traitent des données personnelles pour votre compte doivent également se conformer aux normes de protection des données. Nous vous suggérons de leur poser les questions suivantes :

- Ont-ils mis en place des pratiques efficaces pour garantir la sécurité du réseau et des informations, la confidentialité et la protection des données ?
- Se conforment-ils à des normes mondialement reconnues et contrôlent-ils leur conformité ?
- Comment peuvent-ils rendre compte d'une culture de la confiance et de la sécurité ? Quels contrôles proposent-ils pour vous aider à gérer vos données et à respecter vos obligations en tant que contrôleur ?

Dropbox : protection des données

La relation que nous entretenons avec des millions de personnes et d'entreprises à travers le monde est basée sur la confiance.

Nous sommes très reconnaissants de celle que vous nous accordez et nous prenons très au sérieux la responsabilité qui est la nôtre de protéger vos informations. Afin de mériter votre confiance, nous avons conçu et continuons de développer Dropbox en mettant l'accent sur la sécurité, la conformité et la confidentialité.

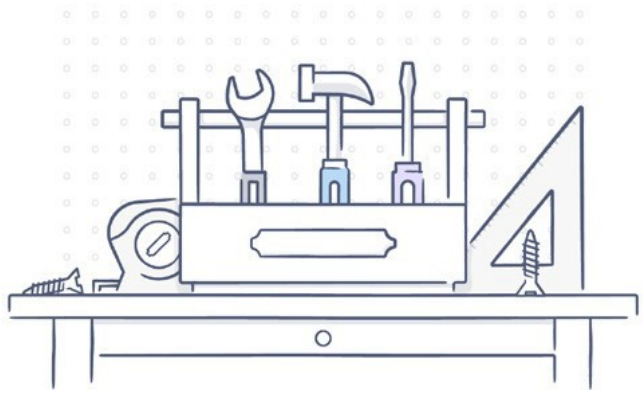
Sécurité : protection et contrôle

Protéger : sécurité des informations et de l'architecture

De par sa conception, Dropbox intègre plusieurs niveaux de protection répartis sur une infrastructure évolutive et sécurisée, notamment : le transfert de données sécurisé, le chiffrement, la configuration réseau et les contrôles au niveau des applications. Par ailleurs, Dropbox a mis en place un cadre régissant la sécurité des informations pour évaluer les risques et développer une culture de la sécurité au sein de l'entreprise. À ce titre, nous vérifions et mettons à jour régulièrement nos règles de sécurité, nous formons nos collaborateurs aux questions de sécurité, nous testons la sécurité de nos applications et de notre réseau (notamment via des tests de pénétration), nous surveillons la conformité aux règles de sécurité, et nous réalisons des évaluations des risques. Vous trouverez les informations complètes dans notre livre blanc sur la sécurité de Dropbox Business.

Contrôler : donner plus de pouvoir aux administrateurs informatiques

Dropbox fournit aux administrateurs informatiques les fonctionnalités de contrôle et de visibilité dont ils ont besoin pour mieux gérer vos obligations de conformité. Notre tableau de bord d'administration permet de surveiller l'activité du compte, d'afficher les appareils connectés et d'effectuer un audit des activités de partage. Créez des groupes pour gérer facilement l'accès des membres de l'équipe à des dossiers spécifiques. Utilisez le gestionnaire de dossiers d'équipe pour profiter d'une visibilité et d'un contrôle accrus sur les dossiers d'équipe, et gérer leur synchronisation. Les contrôles de partage des liens vous permettent de protéger vos liens partagés avec un mot de passe, de limiter la période d'accès avec un délai de validité, et de limiter l'accès aux membres de votre entreprise. Notre outil de transfert de compte vous permet de transférer facilement des fichiers d'un utilisateur à un autre en cas d'évolution de poste. L'effacement à distance vous permet de supprimer les fichiers sur les appareils perdus ou volés.



Conformité : confiance et contrôle

La conformité permet de valider efficacement la fiabilité d'un service. Nous vous encourageons à vérifier la conformité de nos pratiques de sécurité aux réglementations et aux normes les plus reconnues, telles que ISO 27001, 27017, 27018 et SOC 1, 2 et 3. Dans la mesure du possible, nous partageons avec vous les rapports et les avis des auditeurs tiers indépendants chargés de tester nos contrôles. Vous trouverez plus d'informations sur les normes qui s'appliquent à notre entreprise et les procédures de vérification de nos pratiques de sécurité sur notre page dédiée à la conformité.

Confidentialité : notre engagement

Vos données vous appartiennent et qu'elles soient personnelles ou professionnelles, nous accordons la plus grande importance à la confiance que nous accordent nos utilisateurs et nous nous engageons à garantir la sécurité de toutes les données enregistrées dans nos systèmes. Nous vous invitons à consulter notre politique de confidentialité pour comprendre comment nous traitons et protégeons vos informations. Nous publions également un rapport de transparence et des principes relatifs aux demandes émanant des autorités pour partager la fréquence à laquelle nous recevons, examinons et répondons à ces demandes, et nous tentons également de modifier les lois en vue de mieux protéger votre vie privée.

Préserver ensemble la sécurité de vos données

Dropbox travaille avec ses clients pour protéger leurs données. Nous prenons des mesures complètes afin de protéger notre infrastructure, notre réseau et nos applications ; former nos employés aux pratiques de sécurité et de confidentialité ; développer une culture où être digne de votre confiance est notre priorité absolue ; et faire évaluer nos systèmes et pratiques par des audits et tests rigoureux menés par des tiers. Nos clients jouent également un rôle clé dans la protection et la sécurisation de leurs équipes et leurs données. Dropbox vous permet de configurer, utiliser et surveiller l'activité de votre compte de façon à répondre aux besoins de votre entreprise en matière de sécurité, vie privée et conformité. Notre guide sur la responsabilité partagée explique les mesures que nous prenons pour protéger votre compte, et ce que vous pouvez faire pour garder le contrôle et de la visibilité sur les données de votre équipe.