Exemple de procédure RGPD : modèle prêt à l'emploi

Cette ressource vous fournit un exemple de procédure RGPD complet et adaptable. Vous y trouverez un modèle de document à copier, des consignes pour le personnaliser, et une checklist pour vous assurer de couvrir les points essentiels de la conformité.

Ce document est un modèle générique et ne constitue pas un avis juridique. Pour une conformité complète, consultez un avocat spécialisé en protection des données ou votre DPO. Adaptez le contenu à votre organisation et à vos traitements.

Mode d'emploi

1. Téléchargez le modèle de procédure RGPD vierge ou copiez le texte ci-dessous.
2. Personnalisez chaque section avec les informations de votre organisation.
3. Identifiez vos traitements de données et remplissez le registre des activités.
4. Diffusez la procédure auprès de vos équipes et assurez-vous de sa mise en œuvre.
5. Révisez régulièrement la procédure pour rester en conformité.

Objectif d'une procédure RGPD

Une procédure RGPD a pour but de définir les étapes à suivre pour garantir la protection des données personnelles au sein d'une organisation. Elle couvre la collecte, le traitement, le stockage et la suppression des données, ainsi que la gestion des droits des personnes.

Contenu du modèle

Le modèle ci-dessous comprend les sections principales : champ d'application, définitions, principes de protection, registre des activités, droits des personnes, gestion des violations, et mesures de sécurité.

Modèle prêt à adapter

PROCÉDURE RGPD - [Nom de votre organisation] 1. Objet Cette procédure définit les règles de traitement des données personnelles au sein de [Nom de l'organisation] afin de se conformer au Règlement Général sur la Protection des Données (RGPD). 2. Champ d'application Cette procédure s'applique à tous les employés, sous-traitants et partenaires traitant des données personnelles pour le compte de [Nom de l'organisation]. 3. Définitions - Donnée personnelle : toute information se rapportant à une personne physique identifiée ou identifiable. - Traitement : toute opération portant sur des données personnelles (collecte, enregistrement, conservation, etc.). - Responsable de traitement : l'entité qui détermine les finalités et les moyens du traitement. - Sous-traitant : l'entité qui traite des données pour le compte du responsable. 4. Principes de protection des données - Licéité, loyauté et transparence - Limitation des finalités - Minimisation des données - Exactitude - Limitation de la conservation - Intégrité et confidentialité 5. Registre des activités de traitement Le registre est tenu à jour par [Nom du DPO ou responsable]. Il comprend pour chaque traitement : - Finalité - Catégories de personnes concernées - Catégories de données - Destinataires - Durée de conservation - Mesures de sécurité 6. Droits des personnes Les personnes concernées peuvent exercer leurs droits : accès, rectification, effacement, limitation, portabilité, opposition. Toute demande doit être traitée dans un délai d'un mois. 7. Gestion des violations de données En cas de violation, le responsable de traitement doit notifier la CNIL dans les 72 heures si la violation présente un risque pour les droits et libertés des personnes. Les personnes concernées doivent être informées si le risque est élevé. 8. Mesures de sécurité - Contrôle des accès - Chiffrement des données - Sauvegardes régulières - Sensibilisation du personnel 9. Révision Cette procédure est revue au moins une fois par an ou en cas de changement réglementaire.

Checklist

[ ] Nommer un DPO si nécessaire

[ ] Tenir un registre des activités de traitement

[ ] Mettre en place des mesures de sécurité techniques et organisationnelles

[ ] Informer les personnes sur leurs droits

[ ] Établir une procédure de gestion des violations

[ ] Former le personnel au RGPD

[ ] Réaliser des analyses d'impact si nécessaire

[ ] Signer des contrats avec les sous-traitants

[ ] Vérifier la conformité des transferts hors UE

[ ] Documenter les décisions et les actions

Questions fréquentes

Qui est concerné par le RGPD ?

Toute organisation, publique ou privée, qui traite des données personnelles de résidents de l'Union européenne, quel que soit son pays d'implantation. Les obligations varient selon la taille et la nature des traitements.

Qu'est-ce qu'une violation de données ?

Une violation de données est une brèche de sécurité entraînant accidentellement ou illicitement la destruction, la perte, la modification, la divulgation non autorisée ou l'accès à des données personnelles. Elle doit être notifiée à la CNIL dans les 72 heures si elle présente un risque.

Dois-je obligatoirement nommer un DPO ?

La nomination d'un Délégué à la Protection des Données (DPO) est obligatoire pour les autorités publiques, les organisations dont l'activité de base consiste en un suivi régulier et systématique à grande échelle, ou le traitement à grande échelle de données sensibles. Dans les autres cas, elle est facultative mais recommandée.