Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une étude d'impact sur la protection des données (en anglais, Privacy Impact Assessment ou PIA).

L'étude d'impact sur la protection des données permet :

- **de bâtir** un traitement de données personnelles ou un produit respectueux de la vie privée,
- **d'apprécier** les impacts sur la vie privée des personnes concernées,
- **de démontrer** que les principes fondamentaux du règlement sont respectés.

Quand mener une étude d'impact sur la protection des données (PIA) ?

- avant de collecter des données et de mettre en œuvre le traitement,
- sur tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques.

Que contient une étude d'impact sur la protection des données (PIA) ?

- **une description** du traitement et de ses finalités,
- **une évaluation** de la nécessité et de la proportionnalité du traitement,
- **une appréciation** des risques sur les droits et libertés des personnes concernées,
- **les mesures envisagées** pour traiter ces risques et se conformer au règlement.

Les outils pour vous aider

La CNIL met à votre disposition sur son site les guides PIA, catalogues de bonnes pratiques qui vous aide à déterminer les mesures proportionnées aux risques identifiés, en agissant sur :

- **les « éléments à protéger »** :
  minimiser les données, chiffrer, anonymiser, permettre l'exercice des droits, etc.
- **les « impacts potentiels »** :
  sauvegarder les données, tracer l'activité, gérer les violations de données etc.
- **les « sources de risques »** :
  contrôler les accès, gérer les tiers, lutter contre les codes malveillants etc.
- **les « supports »** :
  réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier etc.

Pour traiter un risque identifié et le réduire à un niveau acceptable, l'utilisateur des guides peut sélectionner une ou plusieurs mesures appropriées. Il est impératif d'adapter les mesures au risque et au contexte particulier du traitement considéré. Des études de cas sur la géolocalisation de véhicules d'entreprise et la gestion des patients d'un cabinet de médecine du travail, réalisées par le Club EBIOS, illustrent la mise en application de ces outils.

Sur cnil.fr
Pour expérimenter la méthodologie du PIA, téléchargez les guides PIA de la CNIL.

Vous aurez franchi cette étape si :

- ☐ vous avez mis en place des mesures permettant de répondre aux principaux risques et menaces qui pèsent sur la vie privée des personnes concernées par vos traitements.