# Une analyse d’impact (PIA) est-elle obligatoire pour un dispositif de contrôle ?

## Réponse courte

La réalisation d’une analyse d’impact (PIA) est **obligatoire** pour un dispositif de contrôle dès lors que le traitement envisagé est susceptible d’entraîner un risque élevé pour les droits et libertés des personnes concernées, notamment dans le cas de dispositifs de surveillance systématique (vidéosurveillance, géolocalisation, contrôle des accès, etc.) ou de traitements de données sensibles ou à grande échelle.

La CNPD publie une liste des traitements nécessitant un PIA, qui inclut la plupart des dispositifs de contrôle automatisés des salariés. L’absence de PIA en cas d’obligation expose l’employeur à des sanctions administratives.

Le PIA doit être réalisé **avant la mise en œuvre** du dispositif, documenté et conservé, et il doit être présenté à la CNPD en cas de contrôle. Si le PIA révèle un risque élevé non maîtrisé, la consultation préalable de la CNPD est obligatoire.

## Définition

L’analyse d’impact relative à la protection des données (PIA) est une procédure formalisée visant à évaluer, avant la mise en œuvre d’un traitement, les risques que ce traitement fait peser sur les droits et libertés des personnes concernées. Elle s’applique aux traitements susceptibles d’engendrer un risque élevé pour les droits et libertés des salariés, notamment lors de l’installation de dispositifs de contrôle tels que la vidéosurveillance, la géolocalisation ou le contrôle des accès.

Le PIA permet d’identifier les mesures techniques et organisationnelles appropriées pour garantir la conformité du traitement au regard du droit à la protection des données à caractère personnel. Il constitue un outil de responsabilisation du responsable du traitement et de traçabilité des choix opérés.

## Conditions d’exercice

La réalisation d’un PIA est obligatoire lorsque le traitement envisagé est susceptible d’entraîner un risque élevé pour les droits et libertés des personnes concernées, conformément à l’article 35 du Règlement (UE) 2016/679 (RGPD) et à l’article 63 de la loi du 1er août 2018. Sont notamment concernés :

- Les dispositifs de surveillance systématique et régulière d'une zone accessible à un nombre important de salariés (ex : vidéosurveillance sur le lieu de travail).
- Les dispositifs de suivi systématique des activités des salariés (ex : géolocalisation, contrôle des accès informatiques).
- Les traitements de données sensibles ou à grande échelle, ou impliquant un croisement de données multiples.

La CNPD publie une liste des traitements nécessitant un PIA, incluant la plupart des dispositifs de contrôle automatisés des salariés. L'absence de PIA en cas d'obligation expose l'employeur à des sanctions administratives.

## Modalités pratiques

Le PIA doit être réalisé avant la mise en œuvre du dispositif de contrôle. Le responsable du traitement doit :

- Décrire le traitement envisagé, ses finalités, et les moyens techniques et organisationnels mis en œuvre.
- Évaluer la nécessité et la proportionnalité du dispositif au regard de la finalité poursuivie.
- Identifier et apprécier les risques pour les droits et libertés des personnes concernées.
- Déterminer les mesures envisagées pour atténuer ces risques.

Le PIA doit être documenté, daté et conservé afin de pouvoir être présenté à la CNPD en cas de contrôle. Si le PIA révèle un risque élevé non maîtrisé, le responsable du traitement doit consulter la CNPD avant toute mise en œuvre (article 36 RGPD, article 64 loi du 1er août 2018).

## Pratiques et recommandations

Il est recommandé d'associer le délégué à la protection des données (DPO) dès la phase de conception du dispositif de contrôle. L'information préalable et claire des salariés, ainsi que la consultation des représentants du personnel, sont des obligations légales (articles L.261-1 et suivants du Code du travail).

La CNPD met à disposition des modèles et guides méthodologiques pour la réalisation des PIA. Il est conseillé de réévaluer périodiquement le PIA, notamment en cas de modification substantielle du dispositif ou de l'environnement juridique. L'égalité de traitement, la minimisation des données et l'encadrement humain des dispositifs automatisés doivent être garantis.

## Cadre juridique

- Article 35 et 36 du Règlement (UE) 2016/679 (RGPD)
- Loi du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel : articles 63 et 64
- Code du travail luxembourgeois : articles L.261-1 à L.261-4 (dispositifs de surveillance et information/consultation du personnel)
- Décisions et lignes directrices de la CNPD (notamment la liste des traitements nécessitant un PIA)
- Principes généraux de non-discrimination et d'égalité de traitement (article L.241-1 du Code du travail)

La réalisation d'un PIA ne dispense pas l'employeur de respecter l'ensemble des obligations en matière de protection des données, notamment l'information transparente des salariés, la limitation des finalités, la sécurité des données, la traçabilité des traitements et l'encadrement humain des dispositifs automatisés.