L’analyse d’impact sur la protection des données (AIPD)

L’obligation de réaliser une AIPD pour les établissements utilisant l’outil d’aide à la décision

L'OBLIGATION DE RÉALISER UNE AIPD

La CNIL a considéré dans sa « Foire aux questions Informatique et Libertés » sur Parcoursup et les établissements d'enseignement supérieur diffusée le 26 décembre 2018 que :

L'OBLIGATION DE RÉALISER UNE AIPD

En tant que responsables de traitement, les établissements d'enseignement supérieur doivent-ils réaliser une analyse d'impact sur la protection des données (AIPD) ?

Oui.

De manière générale, la réalisation d'une AIPD constitue une bonne pratique facilitant la démarche de mise en conformité des responsables de traitements. La réalisation d'une telle analyse doit en effet permettre d'identifier les risques liés à la mise en œuvre du traitement, de les analyser, de les estimer, de les évaluer, de les traiter, le tout devant s'inscrire dans le cadre d'un processus de réévaluation régulière.

Par ailleurs, une AIPD est obligatoire pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes physiques.

Dans ses lignes directrices sur le sujet, le G29, groupe des « CNIL » européennes, a identifié plusieurs critères aidant à déterminer si le traitement est susceptible d'engendrer un tel risque (notamment l'évaluation ou la notation – y compris le profilage – des personnes concernées, les traitements empêchant de bénéficier d'un droit ou d'un service, etc.). De manière générale, les traitements qui remplissent au moins deux de ces critères doivent faire l'objet d'une analyse d'impact.

Au regard des critères établis par le G29, chacun des traitements mis en œuvre par les établissements d'enseignement supérieur pour classer les candidatures dans ses différentes filières nécessite en principe la réalisation d'une AIPD.

En tout état de cause, une telle analyse qui ne devra pas obligatoirement être transmise à la CNIL ne sera pas immédiatement exigée pour les traitements qui ont fait l'objet d'une formalité préalable avant le 25 mai 2018 ou qui ont été inscrits au registre d'un correspondant informatique et libertés (CIL), sauf en cas de modification substantielle de celui-ci par la suite.

Le RGPD imposant une réévaluation dynamique des risques, les établissements d'enseignement supérieur ayant déclaré leurs traitements avant le 25 mai devront, dans un délai de trois ans, avoir effectué une AIPD.

Qu’est ce qu’une AIPD ?

QU'EST-CE QU'UNE AIPD ?

- **L'article 35 du RGPD prévoit que :**

  - Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

QU'EST-CE QU'UNE AIPD ?

- **Cette analyse d'impact est requise quand** le traitement est « **susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées** » mais aussi lorsque :

  - le traitement figure dans la **liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de réaliser une analyse d'impact** relative à la protection des données

  - le traitement rem**plit au moins deux des neuf critères issus des lignes directrices du G29** :

    - ✓ évaluation/scoring (y compris le profilage) ;
    - ✓ décision automatique avec effet légal ou similaire ;
    - ✓ surveillance systématique ;
    - ✓ collecte de données sensibles ou données à caractère hautement personnel ;
    - ✓ collecte de données personnelles à large échelle ;
    - ✓ croisement de données ;
    - ✓ personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
    - ✓ usage innovant (utilisation d'une nouvelle technologie) ;
    - ✓ exclusion du bénéfice d'un droit/contrat.

La rédaction de l'AIPD « Outil d'aide à la décision »

LE CONTENU D'UNE AIPD

L'AIPD se décomposera en quatre parties :

1. Une description détaillée du traitement mis en œuvre
2. Une évaluation de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux
3. Une étude des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) et de leurs impacts potentiels sur la vie privée des personnes concernées
4. Une description des mesures envisagées pour faire face à ces risques

LA DESCRIPTION DÉTAILLÉE DU FONCTIONNEMENT DU TRAITEMENT

Présenter la nature, la portée, le contexte et les finalités du traitement

Présenter les données à caractère personnel concernées, des destinataires et la durée pendant laquelle les données à caractère personnel seront conservées

Décrire l'opération de traitement

Identifier les actifs sur lesquels reposent les données à caractère personnel

L'EVALUATION DE LA NÉCESSITÉ ET DE LA PROPORTIONNALITÉ DU TRAITEMENT

■ **Présenter les mesures envisagées pour assurer la conformité au règlement :**

➢ **Mesures contribuant au respect des principes de proportionnalité et de nécessité du traitement et fondées sur les exigences :**

- ✓ De licéité du traitement ;
- ✓ D'adéquation, de pertinence et de limitation des données ;
- ✓ De limitation de la durée de conservation.

➢ **Mesures contribuant au respect des droits des personnes concernées :**

- ✓ Informations fournies à la personne concernée ;
- ✓ Droit d'accès ;
- ✓ Droit de rectification et droit à l'effacement ;
- ✓ Droit d'opposition et droit à la limitation du traitement ;
- ✓ Relations avec les sous-traitants ;
- ✓ Renvoi au contrat de sous-traitance.

GESTION DES RISQUES POUR LES DROITS ET LIBERTÉS DES PERSONNES CONCERNÉES

- **Evaluer l'origine, la nature, la particularité et la gravité des risques ou, plus spécifiquement, pour chaque risque du point de vue des personnes concernées :**

  - **Modalités de prise en compte des sources de risques ;**
  - **Identification des impacts potentiels sur les droits et libertés des personnes concernées en cas d'incidents (accès illégitime, modification non désirée ou disparition) ;**
  - **Evaluation de la probabilité et la gravité des risques.**

DÉTERMINER LES MESURES ENVISAGÉES POUR FAIRE FACE À CES RISQUES

- **Indiquer toutes les mesures qui ont déjà été prises et qui doivent être prises pour que le risque ne se réalise pas :**

  - **Envisager TOUTES les possibilités (ne pas se censurer)**

  - **Prévoir un calendrier prévisionnel de déploiement des mesures**

LES DÉLAIS DE RÉALISATION DE L'AIPD POUR L'OUTIL D'AIDE À LA DÉCISION

- Extrait de la FAQ « Parcoursup » de la CNIL :

En tout état de cause, une telle analyse qui ne devra pas obligatoirement être transmise à la CNIL ne sera pas immédiatement exigée pour les traitements qui ont fait l'objet d'une formalité préalable avant le 25 mai 2018 ou qui ont été inscrits au registre d'un correspondant informatique et libertés (CIL), sauf en cas de modification substantielle de celui-ci par la suite.

Le RGPD imposant une réévaluation dynamique des risques, les établissements d'enseignement supérieur ayant déclaré leurs traitements avant le 25 mai devront, dans un délai de trois ans, avoir effectué une AIPD.

Jusqu'au 25 mai 2021

Une méthodologie collaborative

LA RÉALISATION D'UNE AIPD CADRE

Préparation d'une « AIPD cadre » :

➡ Création d'un groupe de travail chargé d'affiner la réflexion et la méthodologie de rédaction de l'AIPD

➡ Organisation de trois ateliers, avec la participation de la CNIL, pour :

- Identifier collectivement les sources de risques
- Identifier les impacts potentiels sur les droits et libertés des personnes concernées en cas d'évènement indésirable
- Identifier l'ensemble des mesures de sécurité susceptibles d'être mises en œuvre et adaptées aux risques identifiés

➡ Transmission de cette AIPD aux établissements

MERCI