MANDIL AVOCATS

Réaliser une analyse d'impact sur la vie privée

Fiche n°05 - Février 2020

Le RGPD prévoit la fin de la plupart des obligations en matière de formalités préalables (déclarations et autorisations de la CNIL). En contrepartie, le responsable de traitement doit être en mesure de démontrer à tout moment sa conformité aux exigences du RGPD (principe d'*accountability*).

Pour ce faire, il doit notamment mettre en place un registre des traitements et effectuer des analyses d'impact sur la vie privée (PIA – Privacy Impact Assessment), lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

A savoir — **L'obligation de tenir un registre des traitements de données**

Prévu à l'article 30 du RGPD, le registre participe à la documentation du traitement en permettant aux responsables du traitement et aux sous-traitants de recenser les traitements de données personnelles réalisés. Le registre détaille notamment les parties prenantes, les données traitées, l'utilisation et les destinataires des données, la durée de conservation et les mesures de sécurité.
Le registre est obligatoire pour entreprises de plus de 250 salariés et pour celles réalisant des traitements à titre régulier (gestion RH, prospection…). **En pratique, rares sont les entreprises dispensées de tenir un registre !**

I. Les traitements concernés

Les responsables de traitements effectuant des **traitements susceptibles de présenter un risque élevé** pour les droits et libertés des personnes concernées **sont tenus de réaliser des analyses d'impact** (article 35 du RGPD) lorsque le traitement :

OU

1. Remplit au moins 2 des critères suivants :

Réalisation d'évaluation ou de notation (profilage, scoring…)	**Surveillance/contrôle systématique des personnes concernées**
Traitement de **données sensibles** (origine ethnique, opinion politique, conviction religieuse, appartenance syndicale, donnée génétique ou biométrique) ou **hautement personnelles** (données de localisation, données financières…)	**Prise de décisions automatisées produisant des effets juridiques** ou affectant une personne de manière significative de façon similaire. Ex : rejet automatique et sans intervention humaine d'une demande de carte bancaire par le client d'un établissement bancaire...
Traitement des données à grande échelle (nombre de personnes concernées, volume de données, durée et étendue géographique)	**Traitement de données concernant des personnes vulnérables** (employés, enfants, malades mentaux, etc.).
Croisement de fichiers de données personnelles	**Usage innovant** (nouvelle technologie)

2. Figure sur la liste adoptée par la CNIL

- Traitements de **données de santé** par les établissements de santé ;
- Traitements de données **génétiques ou biométriques** de personnes dites « **vulnérables** » (patients, employés, enfants…) ;
- **Profilage** de personnes physiques à des fins RH ou **surveillance constante** de l'activité d'employés ;
- Traitements ayant pour finalité la gestion **des alertes et des signalements en matière sociale, sanitaire et professionnelle** ;
- Traitements impliquant le **profilage** des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci (**score pour l'octroi d'un crédit, LCLF aux moyens de paiement**…) ;
- Traitements de données de localisation à grande échelle ;
- …

II. Les traitements non concernés

Traitement ne présentant pas de risque élevé pour les droits et libertés des personnes concernées

Traitements figurant sur la liste des exceptions adoptée par la CNIL (gestion RH pour les petites sociétés, gestion des fournisseurs…)

Traitement nécessaire au respect d'une obligation légale ou nécessaire à l'exécution d'une mission d'intérêt public

Traitement (nature, contexte, finalité…) très semblable à un traitement ayant déjà fait l'objet d'une analyse d'impact

Les traitements initiés avant l'entrée en application du RGPD le 25 mai 2018 devront, s'ils se poursuivent, faire l'objet d'une analyse d'impact avant mai 2021 (et avant en cas de changement majeur affectant le traitement (nouvelle technologie…).

III. L'objet de l'analyse d'impact

L'analyse d'impact doit au moins contenir les éléments suivants :

Analyse d'impact

- **Description systématique** des opérations de traitement et des **finalités** du traitement
- **Evaluation juridique de la nécessité et de la proportionnalité** des opérations de traitement au regard des finalités
- **Etude technique des risques** pour les droits et libertés des personnes concernées (accès non autorisé, modification et disparition de données, et leurs impacts potentiels sur la vie privée)
- **Mesures envisagées** pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement
- **Prise en compte de l'avis des personnes concernées** par les données (études, sondages ou enquêtes etc.) et/ou documentation de toute décision qui irait à l'encontre de l'avis reçu ou du non recueil de l'avis

IV. Qui intervient dans la réalisation de l'analyse ?

Intervenants

Juristes, métiers et RSSI du responsable du traitement

Délégué à la protection des données du responsable du traitement

Eventuels sous-traitants (assistance obligatoire)

A noter

Les outils pour réaliser une analyse d'impact

- Les lignes directrices du G29 sur les analyses d'impact du 4 octobre 2017
- Trois guides de la CNIL sur la méthodologie, l'outillage et bonnes pratiques
- Un logiciel libre de la CNIL permettant de réaliser des analyses d'impact
- La norme ISO/IEC 29134 «Privacy impact assessment – Guidelines»

V. L'avis de la CNIL

En cas de **risque élevé résiduel** qui n'a pas pu être suffisamment atténué par les mesures de sécurité prises suite à l'analyse d'impact (chiffrement, pseudonymisation…), le responsable du traitement devra **consulter la CNIL** avant de mettre en œuvre ce traitement (article 36 du RGPD). Il devra lui communiquer l'analyse d'impact effectuée.

La CNIL **rendra un avis** sous 8 semaines (+ 6 semaines en cas de traitement complexe) et **pourra s'opposer au traitement** à la lumière des caractéristiques et des conséquences du traitement sur les droits et libertés des personnes concernées par le traitement.

Deux régimes de formalités à réaliser auprès de la CNIL demeurent, pour des hypothèses très ciblées :

1. **Le régime de l'autorisation préalable pour :**
   - **Les traitements présentant une finalité d'intérêt public.**
   - **Les traitements automatisés dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention.**
2. **Le régime de la demande d'avis sur un projet d'acte réglementaire autorisant un traitement de données de santé.**

MANDIL AVOCATS