Dernière mise à jour le 19 novembre 2018

RGPD, la CNIL publie la liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise

La CNIL vient de publier la liste des 14 types d'opérations de traitement pour lesquelles une analyse d'impact est requise. L'analyse d'impact relative à la protection des données Le ...

Sommaire

La CNIL vient de publier la liste des 14 types d'opérations de traitement pour lesquelles une analyse d'impact est requise.

L'analyse d'impact relative à la protection des données

Le RGPD prévoit qu'une analyse d'impact relative à la protection des données (AIPD) doit être menée quand un traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

Il énonce 3 types de traitements susceptibles de présenter un risque élevé :

- L'évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- Le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et des infractions ;
- La surveillance systématique à grande échelle d'une zone accessible au public.

Le Comité européen de la protection des données (CEPD) a lui-même identifié 9 critères permettant de caractériser un traitement susceptible d'engendrer un risque élevé :

- Les données traitées à grande échelle ;
- Les données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou de santé, données biométriques et données concernant la vie ou l'orientation sexuelle) ou données à caractère hautement personnel (données relatives à des communications électroniques, données de localisation, données financières, etc.) ;
- Les données concernant des personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- Le croisement ou la combinaison de données ;
- L'évaluation/scoring (y compris le profilage) ;
- La prise de décision automatisée avec un effet juridique ou similaire ;
- La surveillance systématique de personnes ;
- Le traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat ;
- L'utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles.

La CNIL considère, de manière générale, qu'un traitement qui rencontre au moins 2 de ces critères doit faire l'objet d'une AIPD.

La liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise

Le RGPD imposant aux autorités de contrôle d'établir et de publier une liste des 14 types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, la CNIL a établi cette liste par délibération du 11 octobre 2018 :

- Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes : collecte de données sensibles / personnes dites « vulnérables ».
- Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.) : collecte de données sensibles / personnes dites « vulnérables ».
- Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines : évaluation ou notation / personnes dites « vulnérables ».
- Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés : personnes dites « vulnérables » / surveillance systématique.
- Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire : personnes dites « vulnérables » / évaluation ou notation / collecte de données sensibles.
- Traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle : personnes dites « vulnérables » / évaluation ou notation / collecte de données sensibles.
- Traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre : collecte de données sensibles / personnes dites « vulnérables ».
- 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 : évaluation ou notation / croisement ou combinaison d'ensembles de données.
- Traitements mutualisés de manquements contractuels constatés, susceptibles d'aboutir à une décision d'exclusion ou de suspension du bénéfice d'un contrat : croisement ou combinaison d'ensembles de données / prise de décision automatisée avec effet juridique ou effet similaire significatif.
- Traitements de profilage faisant appel à des données provenant de sources externes : évaluation ou notation / croisement ou combinaison d'ensembles de données.
- Traitements de données biométriques aux fins de reconnaissance des personnes parmi lesquelles figurent des personnes dites « vulnérables » (élèves, personnes âgées, patients, demandeurs d'asile, etc.) : collecte de données sensibles / personnes dites « vulnérables ».
- Instruction des demandes et gestion des logements sociaux : collecte de données sensibles / évaluation ou notation.
- Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes : collecte de données sensibles / évaluation ou notation / personnes dites « vulnérables ».
- Traitements de données de localisation à large échelle : collecte de données sensibles / données traitées à grande échelle.

Cette liste est appelée à être régulièrement revue par la CNIL selon son appréciation des « risques élevés » que peuvent présenter certains traitements. Elle ne présente aucun caractère exhaustif.

La CNIL rappelle l'importance des AIPD qui, au-delà de leur caractère obligatoire dans certaines hypothèses et des sanctions encourues en cas de méconnaissance de cette obligation, permettent à chaque responsable de traitement concerné d'identifier les garanties nécessaires afin d'assurer et de démontrer la conformité du traitement qu'il envisage de mettre en œuvre au regard des exigences du RGPD.

Les AIPD sont avant tout l'occasion de mener une réflexion interne, spécifique à chaque traitement, de nature à garantir de manière opérationnelle le respect des principes relatifs à la protection des données et de pouvoir, le cas échéant, le démontrer.

Références

Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, article 35.

Avis 9/2018 du Comité européen de la protection des données du 25 septembre 2018 relatif au projet de liste de l'autorité de contrôle française portant sur les types d'opération de traitements pour lesquelles une analyse d'impact relative à la protection des données (article 35.4 du RGPD).

Délibération CNIL n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD).

Délibération CNIL n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

https://www.legisocial.fr/dossiers-premium/protection-donnees-rgpd.html »