MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE

*Liberté*
*Égalité*
*Fraternité*

# EXEMPLE DE GRILLE D'ÉVALUATION DE LA SENSIBILITÉ D'UN TRAITEMENT

Direction des affaires juridiques – Délégation à la protection des données

Tous les traitements de données à caractère personnel mis en œuvre au sein de nos ministères n'appellent pas nécessairement une analyse juridique circonstanciée de la direction des affaires juridiques (DAJ) pour être inscrits au registre des activités de traitement.

Ainsi, il appartient désormais aux directions et services concernés par la mise en œuvre d'un traitement d'évaluer le niveau de risque de ce traitement pour justifier une saisine de la DAJ.

Les directions et services doivent déterminer ce niveau de risque en se basant sur la grille d'évaluation de la sensibilité du traitement présentée dans ce document.

Seuls les traitements qui seront jugés sensibles au regard des informations renseignées dans cette grille feront l'objet d'une analyse juridique de la DAJ. Les autres traitements ne seront pas analysés par cette dernière.

Il est toutefois indispensable de compléter et de conserver un exemplaire de ce document pour chaque traitement inscrit au registre, y compris ceux ne nécessitant pas l'analyse de la DAJ. Celui-ci permettra en effet de documenter la conformité du traitement au RGPD et à la loi n° 78-17 du 6 janvier 1978, notamment en cas de contrôle de la CNIL.

Si vous rencontrez des difficultés à identifier les risques du traitement que vous envisagez de mettre en œuvre et à compléter ce document, vous être invités à vous rapprocher de votre référent.

# I- Quelles caractéristiques d'un traitement de données à caractère personnel justifient la saisine de la DAJ ?

Quatre caractéristiques peuvent justifier la saisine de la DAJ pour analyse de sa conformité au RGPD et à la loi informatique et libertés, à savoir :

- la présence de données sensibles ;
- la présence d'un algorithme de profilage ou donnant lieu à une prise de décision entièrement automatisée à l'égard des personnes concernées ;
- l'identification d'un risque médiatique ou politique ;
- la nécessité de réaliser une analyse d'impact relative à la protection des données (AIPD).

**Si vous identifiez une seule de ces quatre caractéristiques, il est alors nécessaire de saisir la DAJ.**

Il vous est toutefois demandé de renseigner le présent formulaire dans son intégralité, afin que la DAJ puisse avoir connaissance de l'ensemble des risques inhérents au traitement que vous avez identifiés.

# 1/ Présence de données sensibles

*RAPPEL :*

*Une donnée sensible au sens de l'article 9 du RGPD et de l'article 6 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés est une donnée relative à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, aux données génétiques, aux données biométriques, à la vie sexuelle ou l'orientation sexuelle d'une personne physique ou encore les données relatives à la santé.*

*Il convient de préciser que constitue une donnée de santé toute donnée relative à la santé physique ou mentale d'une personne physique (y compris la prestation de services de soins de santé) qui révèle des informations sur l'état de santé de cette personne. Par exemple : si un traitement mentionne qu'une personne dispose d'un dispositif d'aménagement en braille, il révèle indirectement que la personne est malvoyante ou aveugle. Un tel traitement contient donc une donnée relative à la santé.*

*Le traitement des données sensibles est en principe interdit.*

*Toutefois, le RGPD et la loi du 6 janvier 1978 permettent quelques exceptions à ce principe et prévoient dans certains cas la possibilité de traiter ces données, le cas échéant après la mise en œuvre de certaines formalités*

*Par exemple :*

- *Autorisation de mise en œuvre du traitement par décret en Conseil d'Etat pris après avis de la CNIL ;*
- *Consentement des personnes concernées (étudiants, responsables des élèves, etc). Toutefois, concernant ce point, il convient de rappeler que le RGPD exige la manifestation d'une volonté libre, spécifique, éclairée et univoque des personnes concernées pour qu'elles consentent à la collecte de données sensibles. Or, en pratique, on constate souvent que la collecte de données sensibles sur la base du consentement ne fonctionne pas pour les traitements mis en œuvre par nos ministères. En effet, la plupart du temps, ce consentement n'est pas libre, dans la mesure où son absence pourrait conduire à exclure la personne concernée d'un service ou d'une prestation. Par exemple : un élève en situation de handicap, dont les parents ne consentent pas à la collecte des données de santé dans le cadre d'un traitement de gestion et suivi des élèves en situation de handicap, ne pourrait pas bénéficier du processus d'aide et d'aménagement prévu par ce traitement. Les parents sont donc dans l'obligation de consentir à la collecte des données de santé pour assurer un bon suivi pour leur enfant en situation de handicap, leur consentement ne peut donc pas être considéré comme libre dans ce cas.*

*Ces procédures juridiques complexes imposent une instruction préalable du traitement par la DAJ.*

a) Le traitement que vous envisagez de mettre en œuvre contient-il des données sensibles ?

☐ Non

☐ Oui

b) Si oui, quels types de données contient-il ?

☐ origine raciale ou ethnique

☐ opinions politiques

☐ convictions religieuses ou philosophiques

☐ appartenance syndicale

☐ données génétiques[1]

☐ données biométriques[2]

☐ vie sexuelle ou l'orientation sexuelle

☐ données de santé

c) Selon les cases que vous venez de cocher, **veuillez détailler les données sensibles que vous avez identifiées** (par exemple : handicap, empreinte génétique, appartenance à une communauté religieuse, opinions politiques, etc…) en justifiant brièvement le besoin de traiter cette donnée :

| |
|---|
| |

## 2/ La présence d'un algorithme de profilage ou donnant lieu à une prise de décision automatisée

| |
|---|
| *RAPPEL :*<br><br>*Un algorithme est un ensemble d'opérations automatisées intégrées dans un programme informatique ayant pour but de résoudre un problème et d'obtenir un résultat (Par exemple :* |

[1] Données relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne (AND, génome…)

[2] Données résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique (contour de la main, contour de l'iris, empreintes digitales…).

*un moteur de recherche contient un algorithme qui lui permet d'indexer les résultats les plus pertinents correspondants aux mots recherchés).*

*En d'autres termes, il s'agit de la description d'une suite d'étapes (ou d'instructions) permettant d'obtenir un résultat à partir d'éléments fournis en entrée.*

*Lorsque cet algorithme permet le* ***profilage*** *(construire des profils pour mieux cerner la personnalité, les habitudes ou le comportement d'une personne physique) ou lorsqu'il permet de prendre des* ***décisions entièrement automatisées*** *(décision prise sans aucune intervention humaine important des effets juridiques ou des effets significatifs pour des personnes physiques), alors le traitement en question doit faire l'objet d'une analyse juridique plus approfondie dans la mesure où il peut engendrer des conséquences importantes pour les personnes physiques concernées.*

***Par exemple*** *: le traitement relatif aux mouvements des enseignants actuellement mis en œuvre par notre ministère est susceptible de prendre des décisions entièrement automatisées relatives à la mobilité des agents sans aucune intervention humaine, au sens du RGPD, depuis la suppression des CAP en 2019.*

*Ainsi, si le traitement que vous envisagez de mettre en œuvre inclut un algorithme permettant le profilage ou une prise de décision entièrement automatisée à l'égard des personnes physiques, alors il doit nécessairement faire l'objet d'une saisine de la DAJ.*

a) Le traitement que vous envisagez de mettre en œuvre contient-il un algorithme :

   ☐ Oui

   ☐ Non

b) Si oui, contient-il :

   ☐ un algorithme de profilage

   ☐ un algorithme permettant de prendre des décisions entièrement automatisée

c) Si vous avez coché l'une des cases ci-dessus, veuillez préciser brièvement le fonctionnement de l'algorithme en question et le besoin.

# 3/ L'identification d'un risque politique et/ou médiatique

*RAPPEL :*

*Il appartient aux directions et services de s'interroger sur cette question et d'identifier le/les risque(s) politique(s) et/ou médiatique(s) qu'engendre la mise en œuvre d'un traitement.*

***Par exemple** :*

*De par leur objet, certains traitements font l'objet de l'attention particulière des organisations syndicales, des représentants de parents d'élèves ou de la presse : c'est notamment le cas des traitements relatifs aux évaluations des élèves ou encore ceux relatifs à l'affectation des élèves ou étudiants (par ex. Affelnet et Parcoursup).*

*De la même manière, les enquêtes, dès lors qu'elles concernent les élèves les plus jeunes, font presque systématiquement l'objet d'articles dans les médias (comme par exemple l'enquête relative au confinement du printemps 2020 adressée aux élèves lors des évaluations CP/CE1).*

*Enfin, certains sujets de sociétés, souvent sensibles, comme le harcèlement scolaire, la radicalisation, la violence en milieu scolaire, comportent des risques politiques et/ou médiatiques. Par conséquent, il doit être considéré que tous les traitements relatifs à ces sujets revêtent un caractère sensible justifiant une analyse juridique approfondie de la DAJ.*

Le traitement que vous envisagez de mettre en œuvre présente-t-il un risque politique et/ou médiatique?

☐ Oui

☐ Non

Si oui, le(s)quel(s) ? Veuillez brièvement expliquer le contexte afin de justifier ce(s) risque(s).

# 4/ La nécessité de mettre en œuvre une AIPD

*RAPPEL :*

*L'AIPD doit obligatoirement être mise en œuvre dans trois cas de figure, qui ne sont pas cumulatifs :*

- *le traitement entre dans le champ de l'article 35 du RGPD qui prévoit une liste de traitements pour lesquels une analyse d'impact est requise (a) ;*
- *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 (cf. délibération 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)(b) ;*
- *le traitement remplit au moins deux des neuf critères fixés par la CNIL dans sa délibération n° 2018-326 du 11 octobre 2018 pour déterminer si un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (c).*

*Lorsqu'une AIPD est nécessaire, le traitement révèle un risque important pour les personnes concernées. Il est par conséquent nécessaire qu'il fasse l'objet d'une analyse de la DAJ.*

a) Le traitement que vous envisagez de mettre en œuvre entre-t-il dans le cadre d'une des hypothèses suivantes prévues par l'article 35 du RPGD ?

☐ **l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques**, qui est fondée sur un traitement automatisé, y compris le profilage, 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 catégories particulières de données visées à l'article 9 du RGPD, paragraphe 1, ou de **données à caractère personnel relatives à des condamnations pénales et à des infractions** visées à l'article 10 du RGPD

*Pour information : en l'absence de position claire de la CNIL sur cette question, le critère de la grande échelle s'apprécie relativement à une population donnée (élèves, enseignants, etc..) et au cas par cas. Ainsi, de manière générale, on peut considérer que lorsqu'un traitement concerne l'intégralité des collégiens ou des lycéens de France, le critère du traitement à grande échelle est rempli. En revanche, lorsqu'un traitement concerne uniquement une classe d'âge (par exemple uniquement les sixième), le critère de traitement à grande échelle nous semble pouvoir être écarté, car le nombre d'élèves concernés représente une proportion relative de personnes au regard du nombre total d'élèves. De même, un traitement concernant uniquement les agents de l'administration centrale du ministère ne constitue pas un traitement à grande échelle, quand bien même il concernerait tous les agents de l'administration centrale, dans la mesure où cela représente un très faible nombre au regard de l'ensemble des agents relevant de nos deux ministères.*

☐ la **surveillance systématique** à grande échelle d'une zone accessible au public

b) Le traitement que vous envisagez de mettre en œuvre figure-t-il dans la liste des traitements suivants pour lesquels la CNIL a estimé obligatoire de réaliser une analyse d'impact relative à la protection des données ?

☐ traitement de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes

☐ traitement portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants)

☐ traitement établissant des profils de personnes physiques à des fins de gestion des ressources humaines

☐ traitement ayant pour finalité de surveiller de manière constante l'activité des employés concernés

☐ traitement ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire

☐ traitement ayant pour finalité la gestion des alertes et des signalements en matière professionnelle

☐ traitement des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre

☐ traitement 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

☐ traitement mutualisé de manquements contractuels constatés, susceptibles d'aboutir à une décision d'exclusion ou de suspension du bénéfice d'un contrat

☐ traitement de profilage faisant appel à des données provenant de sources externes

☐ instruction des demandes et gestion des logements sociaux

☐ traitement ayant pour finalité l'accompagnement social ou médico-social des personnes

☐ traitement de données de localisation à large échelle

☐ traitement de données biométriques aux fins de reconnaissance des personnes parmi lesquelles figurent des personnes dites « vulnérables » (élèves, personnes âgées, patients, demandeurs d'asile, etc…)

c) Le traitement que vous envisagez de mettre en œuvre remplit au moins deux des neuf critères suivants fixés par la CNIL ?

☐ 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

*Pour information : Au-delà des dispositions du RGPD, certaines catégories de données peuvent être considérées comme augmentant le risque possible pour les droits et libertés des personnes et sont qualifiées de « données à caractère hautement personnel ». Ce sont par exemple des données financières susceptibles d'être utilisées pour des paiements frauduleux ou des données de localisation dont la collecte met en cause la liberté de circulation des personnes.*

☐ collecte de données personnelles à large échelle
*Pour information : Voir supra les précisions sur ce critère. Cf. a) du 4.*

☐ croisement de données
*Pour information : par exemple, croisement de données issus de deux opérations de traitement de données, ou plus, effectuées à des fins différentes et/ou par différents responsables du traitement, d'une manière qui outrepasserait les attentes raisonnables de la personne concernée.*

☐ personnes vulnérables (employés, personnes âgées, enfants, etc.)
*Pour information : si les employés sont bien reconnus comme des personnes vulnérables, ce critère ne doit pas être retenu du seul fait de la qualité « d'employés » des personnes concernées. Il doit être retenu uniquement lorsque la finalité du traitement suppose un lien de subordination entre l'employeur et l'employer (par exemple : traitement relatif à la surveillance des horaires de travail des employés).*

☐ usage innovant (utilisation d'une nouvelle technologie)
*Pour information : un usage innovant pourrait être un dispositif de reconnaissance faciale ou encore l'utilisation de l'intelligence artificielle*

☐ exclusion du bénéfice d'un droit/contrat

## II- Que faire en présence d'au moins une des quatre caractéristiques ?

Lorsque vous identifiez au moins une des quatre caractéristiques énumérées au I, il est nécessaire de saisir la DAJ et de compléter à cet effet la fiche-type de présentation du traitement.

La fiche-type de présentation doit être adressée à la DAJ accompagnée de la présente grille d'évaluation des risques.

# III-Que faire en l'absence de risque particulier ?

Lorsque le traitement n'engendre aucun risque particulier, il appartient à la direction ou au service chargé de la mise en œuvre de ce dernier de compléter une fiche-registre.

Celle-ci ne fera l'objet d'aucune analyse de la DAJ.

Il convient de préciser que la nécessité de rédiger un acte réglementaire (notamment pour l'information des personnes concernées) ne justifie pas, en elle-même, la saisine de la DAJ. Ainsi, en l'absence de critères de sensibilité, il appartient à chaque direction ou service d'y procéder.

**Nous appelons votre attention sur le fait que cette grille de sensibilité du traitement ne sera examinée par la DAJ que dans le cadre de l'instruction des traitements sensibles. Il apparaît toutefois indispensable de la renseigner pour chaque traitement et de la conserver.**