Conseil national

De :	À :	Objet :
Benoit Gunslay	CNOA + CROA	RGPD

18/04/2018

Les impacts du RGPD sur l'Ordre et la profession

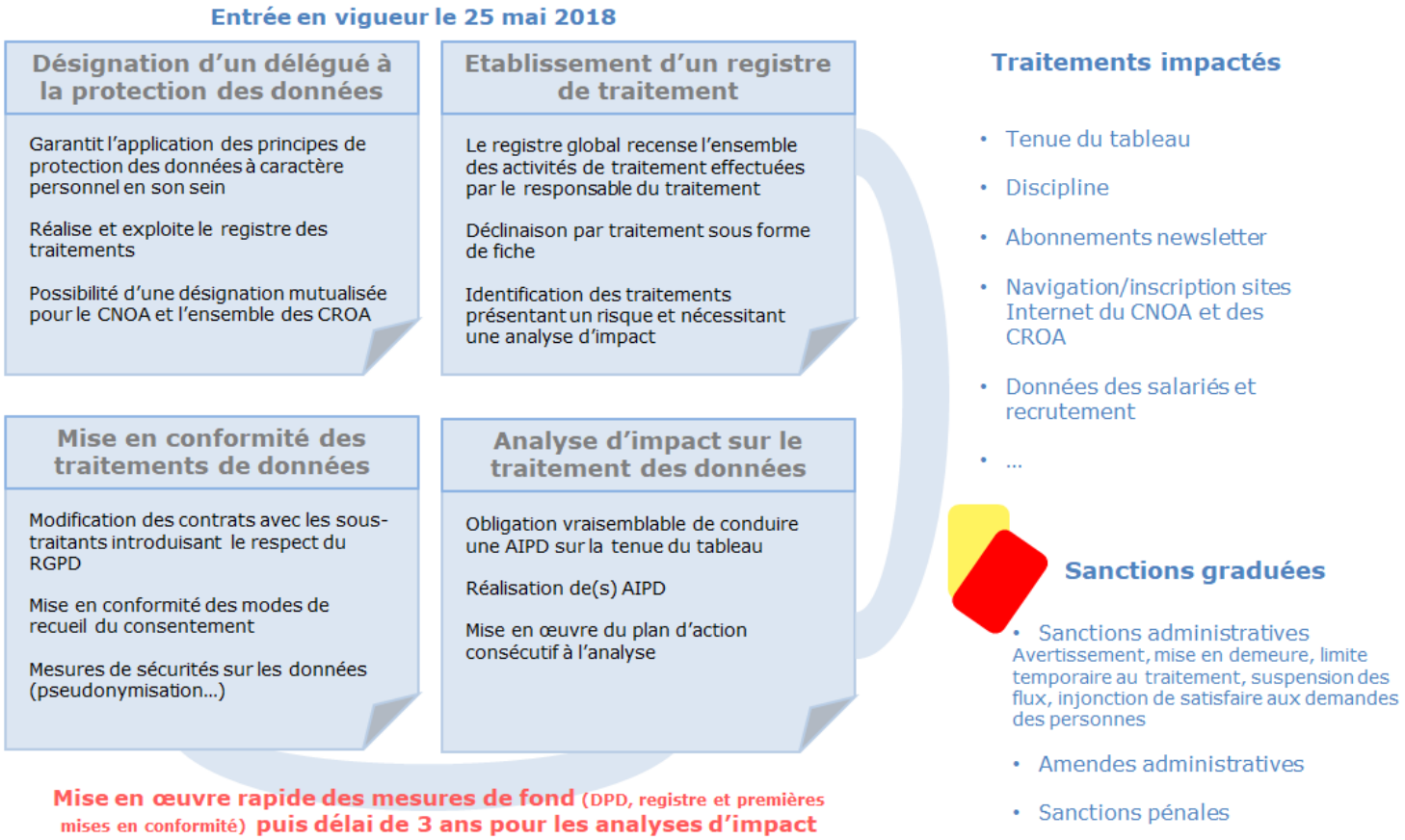
Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données devient le nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel. Il remplace la Directive 95/46/CE sur la protection des données personnelles et entrera en vigueur le 25 mai 2018 dans toute l'Union Européenne.

Conséquence de la mise en œuvre du RGPD, la plupart des formalités préalables actuelles auprès de la CNIL (déclarations, autorisations) vont disparaître, au profit d'une logique de conformité continue. Les organisations qui gèrent, via leurs traitements, des données à caractère personnel devront ainsi prouver que toutes les mesures techniques et organisationnelles ont été mises en œuvre pour les protéger (principe dit d'accountability).

Le RGPD fixe aussi des responsabilités nouvelles au sein des organisations, notamment à travers la désignation d'un délégué à la protection des données (DPD ou DPO selon l'acception anglaise *Data protection officer)*.

De nouveaux outils de conformité sont imposées ou suggérés aux entreprises et organisations : la tenue d'un registre des traitements, la désignation d'un délégué à la protection des données, la notification de failles de sécurité, la certification de traitements, l'adhésion à des codes de conduite, la réalisation d'études d'impact sur la protection des données.

Synthèse des obligations



I - Champ d'application du RGPD

L'enjeu du RGPD est d'encadrer les **traitements**

> *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction*

effectués par un **responsable de traitement**

> *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement*

, ou par un éventuel **sous-traitant** pour son compte,

> *personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement*

sur des **données personnelles.**

> *toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*

Qui est concerné dans le champ de la profession ?

L'application du règlement sur la protection des données ne dépend pas de la taille de l'entreprise ou de l'organisation mais de la nature des activités. Il s'applique potentiellement à toutes les structures, privées ou publiques ayant un établissement dans l'Union Européenne qui effectue un traitement sur des données personnelles.

Le CNOA, les CROA et les entreprises d'architectures rentrent donc dans le champ d'application du RGPD, avec des obligations différenciées selon la nature de l'activité (mission de service public ou activité privée), les circonstances de recueil des données et la finalité de leur traitement (traitement régulier ou occasionnel, données recueillies dans le cadre d'une disposition législative ou dans un cadre contractuel, données recueillies à des fins commerciales), la quantité de données et leur caractère éventuellement sensible.

L'impact du RGPD pèse surtout sur l'Institution. Les traitements de données opérés par les agences restent des activités accessoires, ponctuelles et les données traitées sont a priori dénuées de tout risque pour les droits et de caractère sensible (ce qui différencie les architectes des autres professions réglementées comme les médecins ou avocats notamment). Le RGPD n'impose par ailleurs pas la tenue d'un registre de traitement aux entreprises de moins de 250 salariés. Les agences ne sont pas dispensées de prendre des mesures de fond pour se mettre en conformité mais elles devraient être aujourd'hui limitées à quelques mentions sur leurs sites Internet pour présenter de manière conforme les modalités liées au consentement.

Les éventuels sous-traitants opérant le traitement des données pour le compte des organisations sont également visés par le texte. Il appartient donc au responsable du traitement de vérifier auprès des sous-traitants que leurs activités sont effectuées conformément au RGPD.

II - Grands et nouveaux principes en matière de traitement des données personnelles

- Licéité, loyauté et transparence

> *Les données à caractère personnel doivent être traitées de manière licite, loyale et de manière transparente au regard de la personne concernée.*

- Expression de la finalité du traitement

> *Les données collectées en vue d'un traitement s'inscrivent dans des finalités précisés, déterminés, explicites, légitimes et communiquées à la personne. Elles ne doivent pas être traitées de manière incompatible avec la finalité poursuivie*

- Minimisation des données

> *Elles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées*

- Durée limitée de conservation des données

> *Les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées*

- Exactitude des données

> *Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder*

- Sécurisation des données / Principe d'accountability

> *Les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)*

- Opt-in et opt-out

> L'opt-in, c'est obtenir l'accord de la personne dont on collecte les données : s'il n'a pas dit "oui", c'est "non".
> L'opt-out, c'est lorsque la personne ne s'est pas opposé : si elle n'a pas dit "non", c'est "oui".
>
> Le RGPD renforce l'obtention du consentement auprès des personnes dont on collecte les données. Le consentement consiste en une déclaration ou un acte positif. Il doit être clair et non ambigu pour un traitement spécifique, excluant les consentements par défaut (cases pré-cochées), passifs (opt-out) ou groupés.

- Protection des données dès la conception / protection des données par défaut

> Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Tout nouveau service nécessitant la collecte de données personnes devra donc intégrer le référentiel du RGPD

- Pseudonymisation

> traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

III - Quelles obligations principales naissent du RGPD ?

1/ Désignation d'un délégué à la protection des données

Aux termes de l'article 37 du RGPD, la désignation d'un Délégué sera obligatoire :

- lorsque le traitement est effectué par une autorité publique ou un organisme public
- lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Si le CNOA et les CROA, personnes morales de droit privé exerçant une mission de service public ne relèvent pas légalement de la première catégorie, les pouvoirs publics incitent fortement ces organismes à désigner un DPD[1].

Il fait par ailleurs peu de doute, au regard du nombre d'architectes dont les données sont traitées et de leur nature (infractions disciplinaires intégrées dans le tableau), qu'on puisse associer aux CROA et au CNOA les activités citées au point 2 et 3 de l'article 37 du RGPD

Il est possible de procéder à la désignation d'un DPD mutualisé pour l'ensemble des CROA et du CNOA. Le DPD peut être un salarié ou un prestataire externe. La CNIL recommande de s'assurer des 3 points suivants préalablement à la désignation du DPD :



1. LE DPO DÉTIENT LES COMPÉTENCES REQUISES

Cela suppose :

- une expertise juridique et technique en matière de protection des données personnelles ;
- une bonne connaissance du secteur d'activité, de l'organisation interne, en particulier des opérations de traitements, des systèmes d'information, des besoins en matière de protection et de sécurité des données.

Ces compétences peuvent être acquises, par exemple, à l'occasion de formations adaptées à son profil.

> En savoir plus

2. LE DPO DISPOSE DE MOYENS SUFFISANTS

Cela implique en particulier pour le DPO de :

- disposer du temps suffisant pour exercer ses missions ;
- bénéficier de moyens matériels et humains adéquats ;
- pouvoir accéder aux informations utiles ;
- être associé en amont des projets impliquant des données personnelles ;
- être facilement joignable par les personnes concernées.

> En savoir plus

3. LE DPO A LA CAPACITÉ D'AGIR EN TOUTE INDÉPENDANCE

Cela signifie :

- ne pas être en situation de conflit d'intérêt en cas de cumul de sa fonction de DPO avec une autre fonction ;
- pouvoir rendre compte de son action au plus haut niveau de la direction de l'organisme ;
- ne pas être sanctionné pour l'exercice de ses missions de DPO
- ne pas recevoir d'instruction dans le cadre de l'exercice de ses missions de DPO.

> En savoir plus

Le recours à une prestation de DPO externe représente un cout variable, dépendant du secteur d'activité et des changements imposés sur les traitements.

Une fois choisi, le délégué à la protection des données est désigné en ligne à la CNIL. Celle-ci proposera à l'avenir des mécanismes de certification visant les prestataires externes.

---

[1] Recommandation du GT29 (groupe de travail de l'UE spécifique à l'article 29 du RGPD): Bien qu'il n'y ait pas d'obligation dans ce cas, le G29 recommande, à titre de bonne pratique, que les organismes privés chargés d'effectuer des missions de service public ou exerçant l'autorité publique désignent un DPD.

Pour ce qui concerne les architectes, il ne saurait y avoir une telle obligation. La notion de grande échelle ne semble pas pertinente. Si certaines données sensibles peuvent être potentiellement collectées et faire l'objet d'un traitement, il ne peut s'agir que d'un traitement ponctuel réalisé dans le cadre d'une opération ou de la conclusion d'un contrat.

Certaines professions réglementées ont mis en place des solutions mutualisées (le Conseil national des barreaux a désigné 2 DPO pour l'ensemble des avocats) ou recommandent la désignation d'un DPO (Conseil de l'ordre des experts-comptables) à leurs ressortissants. Les données accessibles aux professionnels du droit et du chiffre sont toutefois bien différentes de celles potentiellement acquises par les architectes. **Il n'y a pas lieu à ce stade de réfléchir à la mise en place d'une solution mutualisée pour le compte des agences** (sur le modèle de ce qui a été fait pour la Médiation de la consommation par exemple, à travers le DPO des architectes)

2/ Mise en conformité des formes de recueil du consentement

Les critères de licéité du traitement de données personnelles évoluent avec le RGPD. Le traitement n'est licite que si au moins une des conditions suivantes est remplie:

> a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
>
> b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
>
> c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
>
> d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
>
> e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
>
> f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

En clair, pour toutes les données collectées par l'Ordre ou par un architecte qui ne rentrent pas respectivement et strictement dans le cadre de la mission de service public, d'une obligation légale (tenue du tableau, conduite de la procédure disciplinaire) ou d'un contrat, le RGPD fixe l'obligation d'obtenir le consentement de la personne concernée.

Le RGPD fait également évoluer les conditions relatives au consentement, défini comme *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;*

L'article 7 fixe les conditions suivantes pour le recueil du consentement :

- Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples.
- La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

A titre d'exemple, les modalités de recueil des données personnelles sur architectes.org au moment de la création d'un compte ne sont pas conformes au RGPD. Les données personnelles communiquées en vue de cet inscription ne reposent ni sur une obligation légale, ni sur la mission de service public de l'ordre et n'entrent pas dans la conclusion d'un contrat.
Actions possibles à réaliser pour se mettre en conformité : créer un champ de formulaire permettant à l'utilisateur de consentir au traitement de ses données personnelles, en indiquant les finalités (bénéficier des fonctionnalités du site, permettre le respect de la charte du site…) ainsi que la durée de conservation des données et en précisant les moyens de se désinscrire. Au titre du principe de minimisation, il faudrait aussi questionner la nature des informations recueillies : le recueil du code postal a-t-il ainsi un intérêt particulier dans les finalités exprimées au départ ?

3/ Etablissement d'un registre de traitement

Le règlement impose prioritairement à toutes les organisations de connaître précisément ses données, la façon dont elles sont traitées, selon quel processus, et par qui/quoi.

Cette obligation se traduit notamment par 2 actions à réaliser :

- **la tenue d'un registre de traitement,** qui recense l'ensemble des activités de traitement effectuées par le responsable du traitement. L'article 30 du RGPD impose qu'y figure :

  - les noms et coordonnées des acteurs **:** responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
  - les finalités du traitement ;
  - la description des catégories de personnes concernées ;
  - les catégories de données à caractère personnel ;
  - les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;
  - le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ;
  - dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
  - dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

La CNIL met à disposition un modèle européen de registre de traitement.

La tenue d'un registre ne **s'impose pas aux organisations qui emploient moins de 250 personnes,** sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9 (données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle)

Par conséquent, l'obligation de tenir un registre s'impose au CNOA et au CROA parce que le traitement de données personnelles, correspondant à la tenue du tableau, fait partie d'une des activités de base de l'Institution.

Il en va différemment pour les agences d'architecture dont le traitement de données personnelles (emploi, données collectées de clients) ne constitue qu'une activité ponctuelle et qui collectent des données non sensibles.

4/ Renforcement des mesures de sécurité liées au traitement des données

4.1/ Mesures techniques et organisationnelles

L'article 32 du RGPD impose au responsable du traitement ainsi qu'aux sous-traitants la mise en œuvre de mesures techniques et organisationnelles appropriées permettant de garantir un niveau de sécurité adaptée aux risques. Les mesures sont de différents ordres :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Les mesures organisationnelles peuvent consister en l'adoption de codes de conduite ou l'insertion dans une démarche de certification des traitements

Le responsable de traitement devra également prendre des mesures afin que tout salarié accédant à des données personnelles y soit expressément autorisé via la formalisation de procédures notamment.

4.2/ Notification à la CNIL d'une violation de données à caractère personnel

Le responsable de traitement doit notifier toute *fuite* relative à des données personnelles à la CNIL dans un délai recommandé de 72 heures après en avoir pris connaissance. Le sous-traitant a un devoir d'information immédiat auprès du responsable de traitement en cas de découverte d'une violation.

La notification doit au minimum :

a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier.

4.3/ Communication à la personne concernée d'une violation de données à caractère personnel

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et reprendre au moins certaines informations (identité du DPD, conséquences probables de la violation) et décrire les mesures prises par le responsable de traitement.

5/ La conduite d'une analyse d'impact sur la protection des données (AIPD)

5.1 / Principe de l'AIPD

Lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement doit conduire une analyse d'impact sur la protection des données (AIPD ou PIA selon l'acronyme anglais).

L'AIPD est une étude aidant à construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD. Elle contient :

- Une description du traitement étudié et de ses finalités.
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités
- une évaluation des risques pour les droits et libertés des personnes concernées les mesures envisagées pour faire face aux risques.

5.2 / Obligation de réaliser une AIPD

L'AIPD est en particulier requise dans les cas suivants:

- 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, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou
- la surveillance systématique à grande échelle d'une zone accessible au public

Il n'est pas obligatoire d'effectuer une AIPD pour chaque opération de traitement. Celle-ci n'est requise que lorsqu'un type de traitement est «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques». Le risque élevé fait l'objet d'une appréciation fondée sur 9 critères :

- Évaluation ou notation
- Prise de décisions automatisée avec effet juridique ou effet similaire significatif
- Surveillance systématique
- Données sensibles ou données à caractère hautement personnel
- Données traitées à grande échelle
- Croisement ou combinaison d'ensembles de données,
- Données concernant des personnes vulnérables (considérant 75):
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles
- Traitements en eux-mêmes qui «empêchent [les personnes concernées] d'exercer un droit ou de bénéficier d'un service ou d'un contrat»

Le GT29 estime que plus le traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une AIPD, quelles que soient les mesures que le responsable du traitement envisage d'adopter.

Le déclenchement d'une AIPD est consécutif à l'établissement du registre de traitement, où le responsable de traitement a l'obligation d'évaluer le degré de risque d'un traitement.

Sauf exception prévue par la CNIL à l'avenir, **le traitement des données du tableau devrait a priori conduire à la réalisation d'une AIPD, pouvant potentiellement être rattaché à 4 des 9 critères précités** : prise de décisions automatisées avec effet juridique ou effet similaire, données sensibles, données traitées à très grandes échelles, croisement ou combinaison d'ensemble de données