PIA : clé de voûte de votre conformité RGPD

Edmond CISSE

Consultant Risk Manager - DPO

PIA : clé de voûte de votre conformité RGPD

Introduction

Règlement 2016/679 (GDPR) sera applicable à partir du 25 mai 2018. Le GDPR introduit concept d'une étude d'impact sur la protection des données (DPIA ou PIA).

Art 35 : « 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. »

PIA : clé de voûte de votre conformité RGPD

Sur quoi porte un PIA ?

Une seule ou un ensemble d'opérations de traitement similaires

Considérant 92 *"… il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée. ".*

PIA : clé de voûte de votre conformité RGPD

Non-respect des exigences du DPIA ?

Une amende administrative pouvant aller jusqu'à 10 M € ou, dans le cas d'une entreprise, jusqu'à 2% du CA total annuel mondial

Défaut de conduite d'un PIA d'un traitement à risque (art. 35(1 et 3))

Conduite incorrecte de la PIA (art. 35(2,7 et 9))

Défaut de consultation de l'autorité de contrôle (art. 36 (3.e)).

PIA : clé de voûte de votre conformité RGPD

PIA obligatoire ?

Traitement " susceptible d'engendrer un risque élevé ".

(a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé individuel;

(b) le traitement à grande échelle de catégories particulières de données, ou relatives à des condamnations pénales et à des infractions;

(c) la surveillance systématique à grande échelle d'une zone accessible au public

…

PIA : clé de voûte de votre conformité RGPD

uræus CONSULT

Traitement à risque élevé ?

Segmentation, profilage et prédiction

En particulier *“visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements…”* (consider. 71 and 91).

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Prise de décisions individuelle automatisée

Les traitements destinés à des prises de décisions sur des personnes concernées produisant des *“des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative.” (Art. 35(3)(a)).*

Par exemple des traitements pouvant conduire à des exclusions ou des discriminations à l’égard de personnes.

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Surveillance systématique

Traitements destinés à observer, surveiller ou contrôler des personnes concernées, y compris la collecte de données via *“la surveillance systématique à grande échelle d'une zone accessible au public ”(Art.* 35(3)(c)).

Ce type de surveillance est un critère car les données personnelles peuvent être collectées dans des circonstances où les personnes concernées peuvent ne pas savoir qui collecte leurs données et comment elles seront utilisées.

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Données à caractère personnel sensibles

Les catégories particulières de données définies et les DCP de condamnations pénales et aux infractions.

Plus généralement, des données qui peuvent être considérées comme augmentant le risque pour les droits et libertés des individus, telles que les données de communication électronique, les données de localisation, les données financières,… « life-logging applications »

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Traitement de DCP à large échelle

Le Règlement ne définit pas le terme “large échelle” mais des indications :

- Nombre absolu de personnes concernées ou pourcentage de la population;
- Volume de données et/ou gammes différentes de données traitées
- Durée/fréquence de l’activité de traitement des données
- Etendue géographique de l’activité de traitement

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Traitement de données agrégées

Par exemple, données provenant de plusieurs opérations de traitement de données ayant des finalités différentes et/ou réalisées par différents responsables de traitement mais, et combinées d'une manière qui outrepasserait les droits et libertés légitimes de la personne concernée.

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Traitement de données de personnes concernées vulnérables

Le traitement de ce type de données peut nécessiter la conduite d'un PIA du fait du *déséquilibre de pouvoir entre les personnes concernées et le responsable de traitement*, avec le risque qu'une personne ne puisse donner son consentement ou s'opposer au traitement des ses données personnelles.

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Traitement basé sur des nouvelles technologies

Les nouvelles technologies peuvent induire de nouvelles formes de collecte et d'utilisation des données, avec un risque élevé pour les droits et libertés des individus et des conséquences personnelles et sociales inconnues.

Ex : Utilisation combinée d'empreintes et de reconnaissance faciale pour améliorer le contrôle des accés physiques

Applications IoT pouvant avoir des impacts significatifs et au quotidien sur la vie privée des personnes.

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Transfert de données hors-UE

Il faut prendre en considération, entre autres, le ou les pays de destination envisagés, la possibilité de nouveaux transferts ou la probabilité de transferts sur la base de dérogations pour des situations spécifiques définies par le GDPR.

PIA : clé de voûte de votre conformité RGPD

Traitement à risque élevé ?

Traitement empêchant l'exercice d'un droit

- Les traitements réalisés dans un espace public que les passants ne peuvent éviter (vidéoprotection)

- Les traitements visant à autoriser, modifier ou refuser l'accès à un service

- La conclusion d'un contrat pour les personnes concernées.

PIA : clé de voûte de votre conformité RGPD

Le PIA est obligatoire ?

Traitement cumulant au moins deux critères

Un traitement qui remplit qu'un seul critère présente un risque de faible niveau

Un traitement qui cumule au moins deux critères doit faire l'objet du PIA.

Plus le nombre de critères cumulés par un traitement est élevé, plus grande sera la probabilité qu'il engendre un risque de haut niveau

Exemple de traitement	Critère applicable	DPIA ?
Un hôpital traitant les données génétiques et de santé de ses patients (Système d'Information Hospitalier)	• DCP sensibles • DCP de personnes vulnérables	OUI
L'utilisation d'un système de caméra pour surveiller le comportement de conduite sur les autoroutes. Le traitement envisage d'utiliser un système intelligent d'analyse vidéo pour identifier les voitures par reconnaissance automatiquement les plaques d'immatriculation.	• Surveillance systématique • Usage innovant et utilisation de solutions technologiques ou organisationnelles	
Une entreprise surveillant les activités de ses employés, y compris poste de travail des employés, l'activité sur Internet, etc.	• Surveillance systématique • DCP de personnes vulnérables	
La collecte de données sur les médias sociaux publics permet aux entreprises privées de générer des profils pour les annuaires de contacts.	• Evaluation ou segmentation • DCP traitées à large échelle	
Un magazine en ligne utilisant une liste de diffusion pour envoyer un résumé quotidien générique à ses abonnés.	• Aucun critère … ?	NON
Un site e-commerce affichant des publicités pour des pièces de voitures anciennes impliquant un profilage limité basé sur le comportement d'achat passé sur certaines parties de son site Web	• Évaluation ou segmentation, mais ni systématique ni à large échelle	

CLUSIR PACA

PIA : clé de voûte de votre conformité RGPD

Le PIA est facultatif ?

- lorsque le traitement n'est pas "susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques" (art. 35 (1));

- lorsque la nature, la portée, le contexte et les finalités du traitement sont très similaires à un traitement pour lequel un PIA a été effectué.

- lorsque la loi réglemente le traitement spécifique et lorsqu'un PIA, conformément aux normes du GDPR, a déjà été réalisé dans le cadre de l'établissement de cette base juridique (art. 35(10);

- lorsque le traitement est inclus dans la liste des opérations de traitement établie par l'AC et pour lesquelles elle statue qu'un PIA n'est pas requis (art. 35(5))

PIA : clé de voûte de votre conformité RGPD

Registre des PIA ?

Un responsable du traitement soumis à l'obligation de réaliser un PIA doit tenir un registre des études d'impacts, comprenant, entre autres, les finalités du traitement, une description des catégories de données et les destinataires des données, et les mesures de sécurité techniques et organisationnelles mises en œuvre.

PIA : clé de voûte de votre conformité RGPD

PIA des traitements existants ?

Traitement post-mai 2018 ou un changement significatif.

- Un PIA est fortement recommandé pour les opérations de traitement déjà en cours avant mai 2018.

- Un PIA doit être conduit au plus tôt en cas de changement du risque présenté par le traitement,

- Un PIA peut également devenir nécessaire lorsque le contexte organisationnel ou sociétal ou de l'activité de traitement a changé,

PIA : clé de voûte de votre conformité RGPD

PIA à quel moment ?

Avant le déploiement du traitement

Le PIA doit être réalisé "avant le traitement" art. 35(1), art. 35(10)

Lors de la conception du traitement même si toutes les opérations du traitement ne sont pas connues.

Le PIA est cohérent avec les principes "de protection lors de la conception et par défaut " (art. 25).

Un PIA doit être continuellement conduit sur les activités de traitement existantes en guise de bonne pratique

PIA : clé de voûte de votre conformité RGPD

Qui doit conduire un PIA ?

Responsable de traitement, sous-traitant avec l'aide du DPO

Le responsable du traitement est responsable du PIA (art.35(2).

Le PIA peut être conduit en interne ou en externe par un consultant Risk manager mais sous le contrôle du responsable de traitement.

Le responsable du traitement doit recueillir l'avis du DPO. Les recommandations et les décisions prises doivent être consignées dans le PIA.

Le DPO est garant de la bonne réalisation du PIA (art.39(1.c))

Si le traitement est effectué en tout ou en partie par un sous-traitant de dernier doit assister le responsable dans le PIA et fournir les informatio

PIA : clé de voûte de votre conformité RGPD

Le PIA doit être publié ?

Oui, en partie ou complet (à l'AC en cas de consultation préalable)

La publication des résultats d'un PIA n'est pas une exigence légale du GDPR mais une telle démarche aiderait à renforcer la confiance des personnes concernées dans les opérations de traitement réalisées et à démontrer la responsabilité et la transparence du responsable de traitement.

PIA : clé de voûte de votre conformité RGPD

Quand consulter l'autorité de contrôle ?

Lorsque les risques résiduels sont élevés

Le *risque résiduel* correspond à la part de risque restant après avoir pris différentes mesures pour réduire le risque principal.

Le risque résiduel élevé est jugé inacceptable dans les cas où les personnes concernées peuvent subir des conséquences importantes, voire irréversibles, qu'elles ne peuvent pas surmonter et/ou lorsqu'il apparaît évident que le risque se réalisera.

Lorsqu'un PIA révèle des risques résiduels élevés, le responsable du traitement doit solliciter une consultation préalable à l'autorité de contrôle (art.36(1)) et devra fourni le PIA de traitement (art.36(3.e))

PIA : clé de voûte de votre conformité RGPD

Le PIA comment ?

Différentes méthodologies mais des critères communs

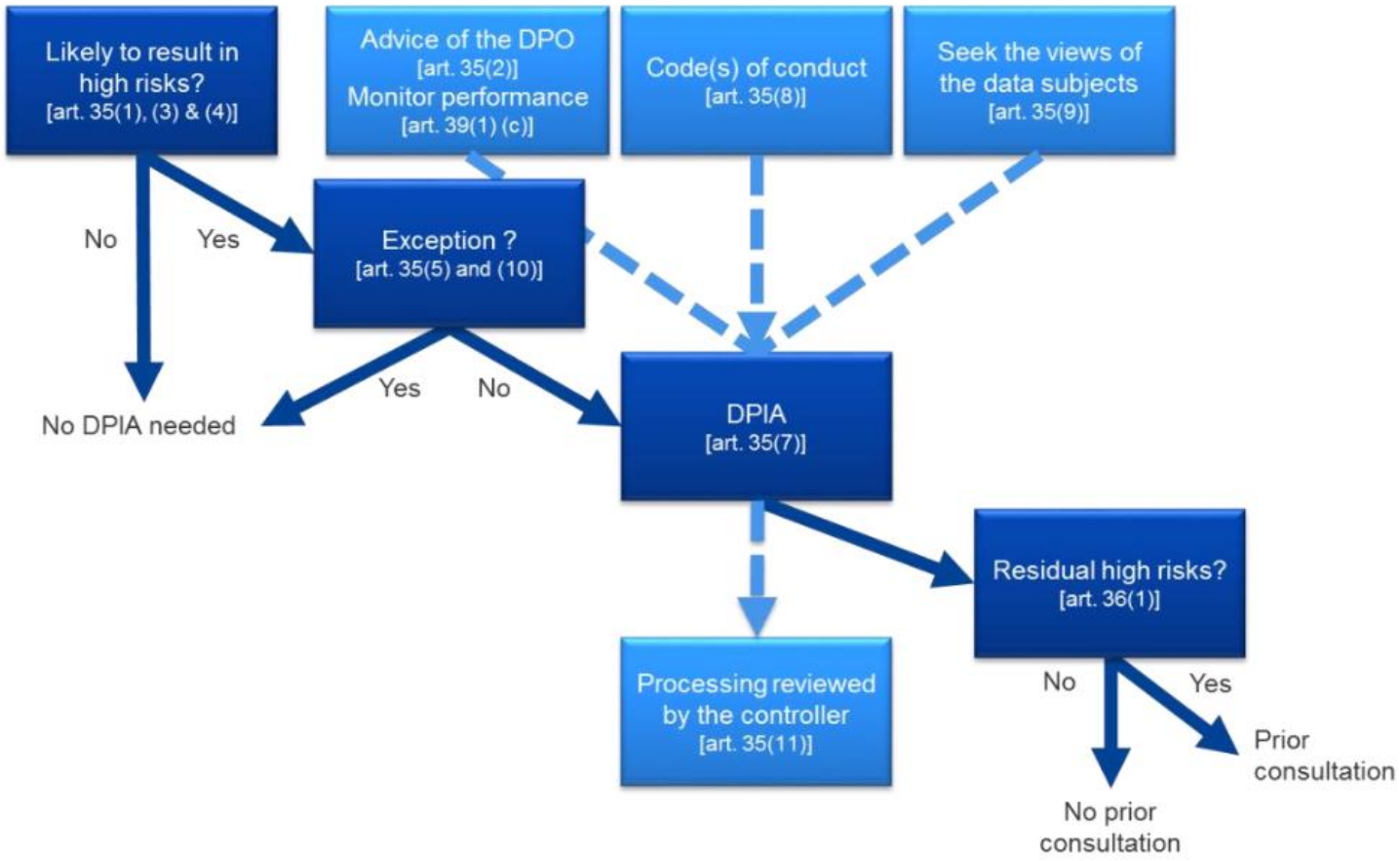
Les caractéristiques minimales d'un PIA :

- Une description des opérations de traitement envisagées et ses finalités
- Une évaluation de la nécessité et de la proportionnalité du traitement
- Une évaluation des risques pour les droits et libertés des personnes

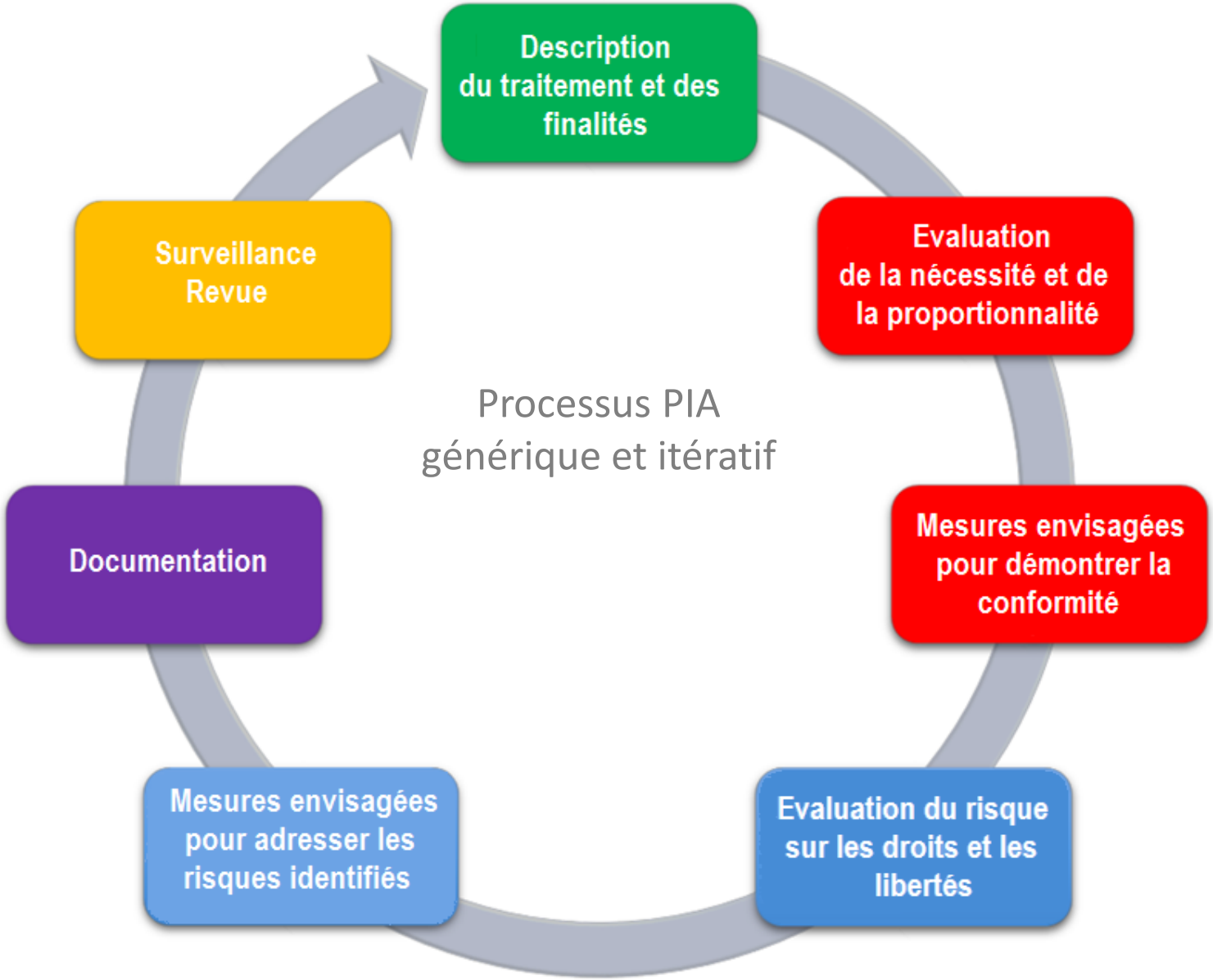
Les mesures envisagées pour:

- Gérer les risques
- Démontrer le respect du Règlement

PIA : clé de voûte de votre conformité RGPD



PIA



CLUSIR PACA

0.

Lancer un nouveau traitement

De nombreux services sont créés tous les jours dans le monde du numérique.

Qu'ils répondent aux besoins internes d'organismes ou à ceux de leurs clients, ces services reposent pour la grande majorité sur des traitements de données à caractère personnel.

Adressés à des groupes d'utilisateurs définis, ils collectent ces données à la volée lors de leur usage.

Stockées sur des serveurs, les données collectées sont vulnérables à différents risques : l'accès illégitime, la modification non désirée et la disparition.

Ces risques sont susceptibles d'avoir un impact important sur la vie privée des utilisateurs concernés.

Source CNIL.FR

1.

Qualifier le traitement

Source CNIL.FR

Ces risques sont indésirables, aussi bien pour le responsable de traitement que pour les utilisateurs du service.

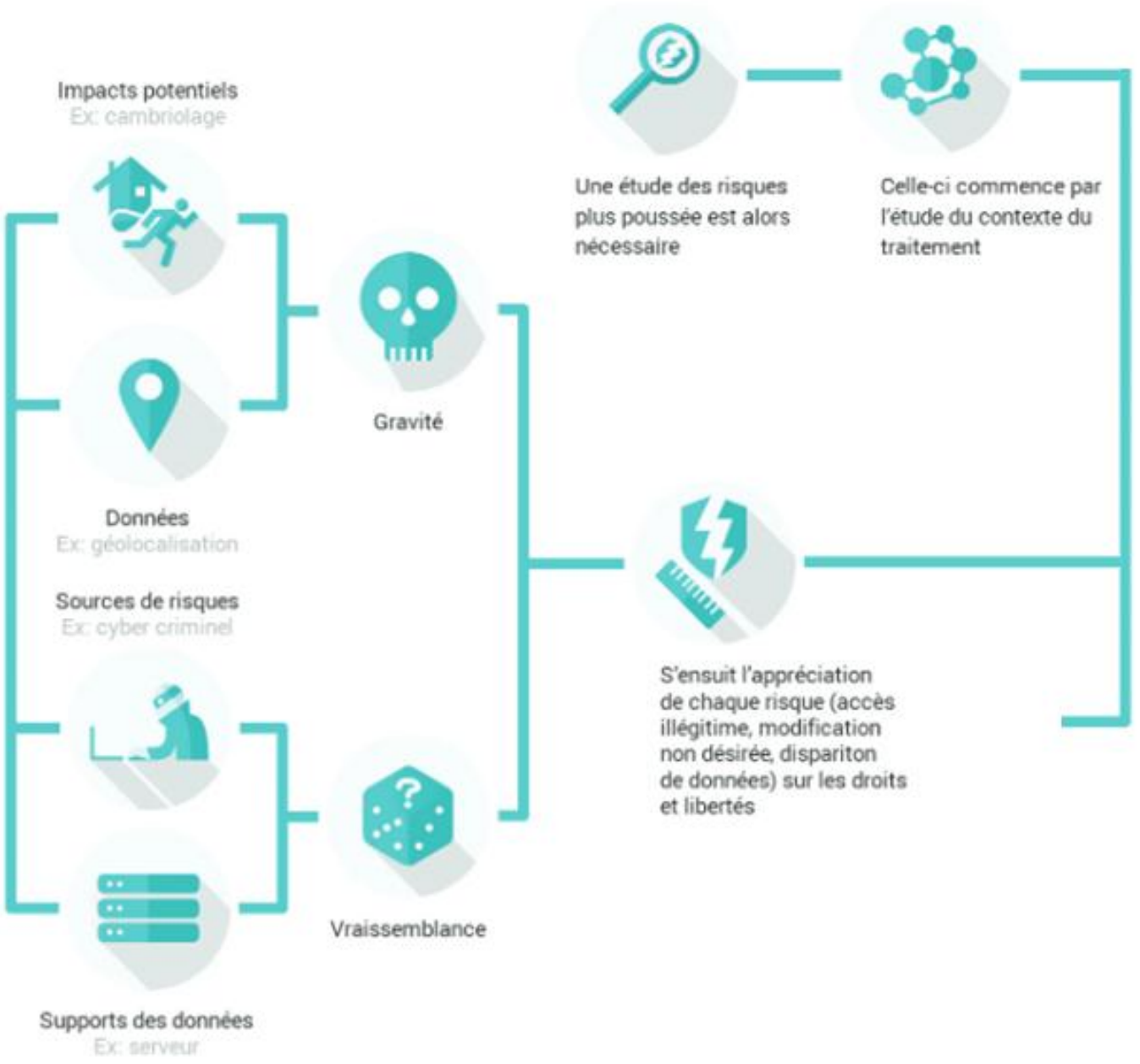
Ainsi, avant de lancer un traitement, il est important d'en faire une première analyse afin d'en déterminer les risques qu'il est susceptible d'engendrer.

Plusieurs facteurs influencent la dangerosité d'un traitement comme par exemple le type de données traité.

En général, si deux des critères listés sont rencontrés, le traitement comporte probablement des risques importants sur la vie privée. Dans ce cas de figure, il est approprié de mener une *« analyse d'impact relative à la protection des données »*.

2.

Apprécier les risques vie privée



L'analyse établit tout d'abord le contexte dans lequel évolue le traitement, en posant, entre autre, les bases de son rôle et de son fonctionnement.

En complément de l'étude juridique consistant à évaluer la nécessité et la proportionnalité du traitement, il est nécessaire d'analyser chaque risque et d'estimer sa vraisemblance et sa gravité selon les impacts potentiels sur les droits et libertés, les données traitées, les sources de risques, et les vulnérabilités des supports de données.

Source CNIL.FR

3.

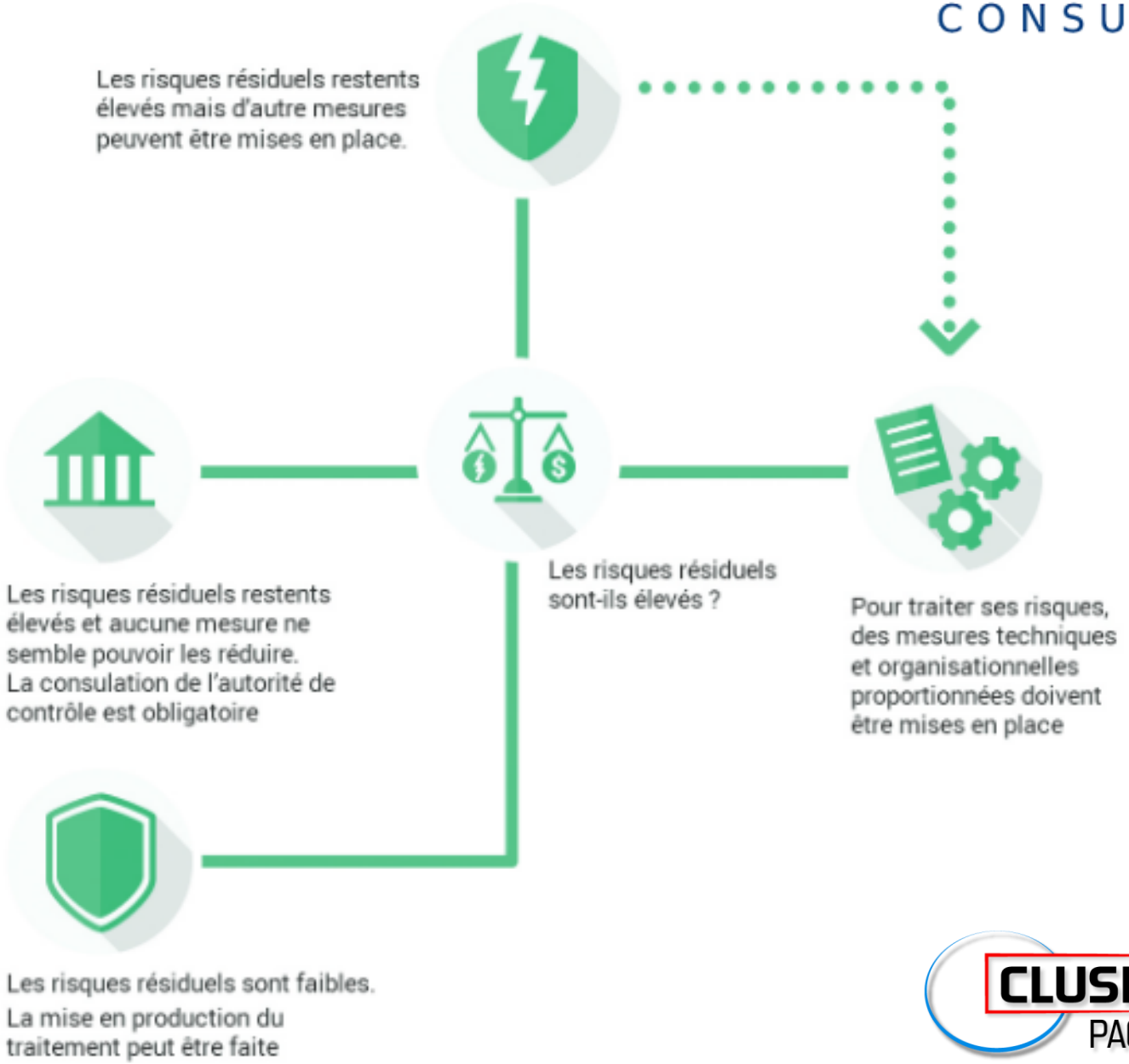
Traiter les risques

Une fois les risques identifiés, des mesures techniques et organisationnelles doivent être déterminées jusqu'à ce que les risques soient réduits à un niveau acceptable.

Si ça ne semble pas possible avec les moyens envisagés, l'autorité de contrôle doit être consultée.

Dans tous les cas, les mesures devront être appliquées avant la mise en œuvre du traitement.

Source CNIL.FR



PIA

Le PIA en action

https://www.cnil.fr/fr/outil-pia-nouvelle-version-beta-du-logiciel