Leto

PRIVACY IMPACT ASSESSMENT (PIA)

TOUT SAVOIR

LETTRE JURIDIQUE

SOMMAIRE

LES POINTS CLÉS

À PROPOS DE LETO

NOTRE HISTOIRE

La protection à la vie privée est gage de transparence et de respect dans la relation avec les autres. Mais la mise en pratique n'est pas toujours simple. Cela peut faire peur.

C'est la raison pour laquelle nous avons créé Leto.

Une solution qui vient concilier simplicité, clarté et efficacité dans le respect des données personnelles d'une entreprise.

POUR NOUS, LA PROTECTION DE LA VIE PRIVÉE EST UN DROIT FONDAMENTAL.

Benjamin Lan Sun Luk et Édouard Schlumberger, fondateurs de Leto

1. INTRODUCTION

Êtes-vous concerné par l’analyse d’impact et quels avantages en retirer pour votre activité ? Suivez notre guide complet.

INTRODUCTION

Dans son rapport annuel de 2021, la CNIL a déclaré plus de 5 000 notifications de violation de données personnelles. Il s'agit d'une augmentation de 79% par rapport à l'année passée. **Ce chiffre est d'autant plus alarmant qu'il doit être revu à la hausse si l'on prend en compte le nombre de violation des données personnelles qui ne sont pas déclarées par les entreprises à la CNIL.**

Ce chiffre signifie que les atteintes portées aux données personnelles des individus augmentent beaucoup plus rapidement que la capacité des acteurs à mettre en place des mesures de sécurités adéquates.

Pour faire face aux risques pesant sur la protection des données personnelles, l'analyse d'impact (PIA) est l'outil le plus efficace pour prévenir toute violation des données personnelles, c'est-à-dire la divulgation, l'altération ou fuite non autorisée des données personnelles (accidentelle ou intentionnelle). Il en va de la protection de la vie privée des personnes et de la réputation de votre entreprise.

Pourtant, le PIA et les règles de protection des données personnelles souffrent d'une grande incompréhension :

1. Le PIA n'est pas un outil complexe à mettre en œuvre. Au contraire, aucun formalisme n'est imposé par le RGPD. Vous êtes libres sur la forme dès lors que les éléments essentiels sont présents : une description du traitement envisagé et des mesures de sécurité adaptées aux risques,
2. Le 100% conforme n'existe pas. Ce qui compte c'est de faire preuve de bonne foi pour se rapprocher de la conformité.

À titre d'illustration, le 10 novembre 2022, la CNIL a prononcé une sanction à l'encontre de la société DISCORD INC "en tenant compte des efforts réalisés par la société pour se mettre en conformité tout au long de la procédure".

En effet, à chaque contrôle, la CNIL est attentive aux efforts fournis et les moyens mis en œuvre par les acteurs pour se conformer au RGPD même si le but n'est pas tout à fait atteint.

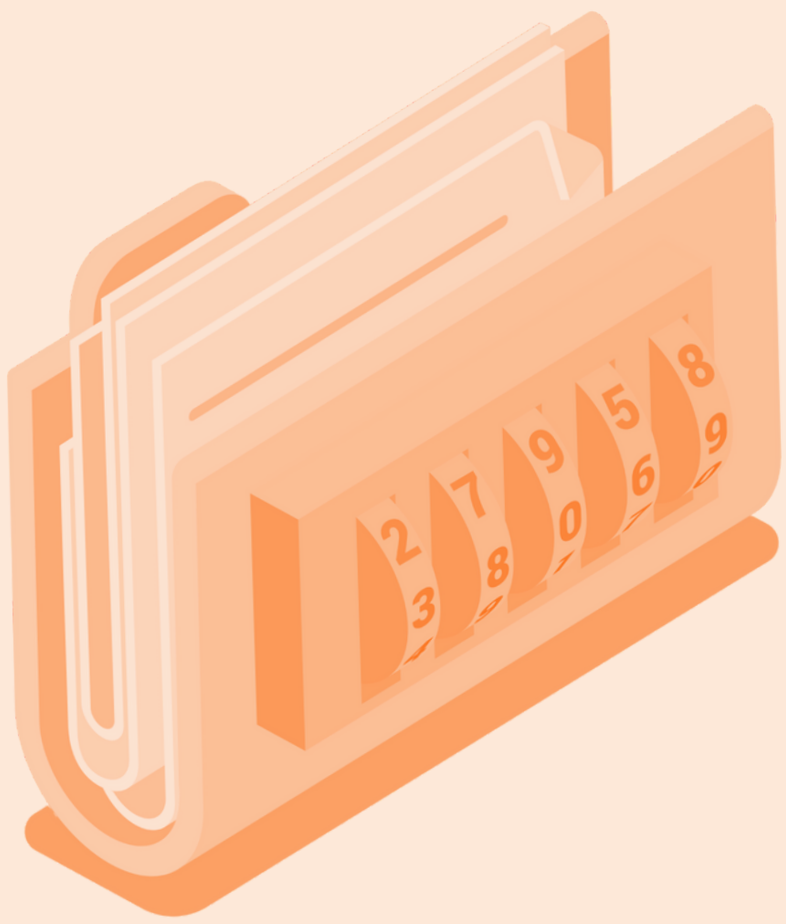
En conséquence, au minimum deux raisons devraient vous conduire à réaliser un PIA :

- Pour votre conformité, il est préférable d'engager la réalisation un PIA, même incomplet, que pas du tout. Il est votre boussole vers la conformité,
- Pour votre activité, le PIA est un élément de réassurance de vos utilisateurs, clients, partenaires et employés. Il constitue un atout concurrentiel majeur pour gagner de nouveaux marchés.

Ce livre blanc a pour objectif de présenter simplement tous les éléments de connaissances dont votre entreprise a besoin pour réaliser une analyse d'impact :

- Qu'est-ce qu'un PIA ?
- Avez-vous l'obligation de réaliser un PIA ?
- Comment réaliser un PIA ?

2. DÉFINITION D'UN PRIVACY IMPACT ASSESSMENT (PIA)



Le PIA vous permet de réduire les risques d'atteinte à la vie privée des personnes.

QU'EST-CE QU'UNE ANALYSE D'IMPACT OU PRIVACY IMPACT ASSESSMENT (PIA)?

D'un point de vue terminologique, on parle d'une **Analyse d'Impact sur la Protection des Données (AIPD) ou en anglais d'une Data Protection Impact Assessment (DPIA) ou encore Privacy Impact Assessment (PIA). Ces trois termes désignent exactement la même chose bien que le terme de PIA soit le plus utilisé.**

En ce qui concerne sa définition, le PIA est une analyse de risque que le responsable de traitement est tenu de réaliser lorsqu'il existe un risque élevé pour les droits et libertés des personnes concernées, en particulier pour la vie privée des personnes.

Pour faire simple, dans le cadre de vos activités, votre entreprise est amenée à traiter des données personnelles, c'est-à-dire collecter et utiliser des données.

Pour rappel, les données à caractère personnel sont toutes les informations se rapportant à une personne physique identifiée ou identifiable directement (par exemple : nom et prénom) ou indirectement (par exemple : le numéro de sécurité sociale, une adresse e-mail, l'enregistrement des conversations) (voir article 4 RGPD).

Dès lors, toutes les données qui permettent de remonter à une personne physique, même indirectement, sont des données à caractère personnel.

Lorsque vous traitez ces données (collecte, utilisation, transmission, destruction de la donnée), le RGPD vous impose un certain nombre d'obligations pour assurer leur protection. Vous avez d'ailleurs à ce titre le rôle de responsable de traitement.

Pour rappel, un responsable de traitement est la personne qui détermine la finalité et les moyens du traitement des données personnelles (article 4 RGPD).

Si l’on reprend la définition du PIA, on comprend que lorsqu’un traitement opéré par le responsable de traitement engendre un risque pour les droits et les libertés des personnes, une analyse d’impact doit être réalisée pour réduire ce risque.

Cette notion de risque est déterminante : le degré de risque détermine si un PIA s’impose et les actions à mener.

Le risque peut être de nature diverse :

- Il peut provenir d’un niveau de sécurité trop faible de nature à engendrer une violation des données personnelles.

Pour rappel, une violation des données à caractère personnel correspond à une violation de leur sécurité entraînant, de manière intentionnelle ou non, la destruction, la perte, la divulgation ou l’accès non autorisé (article 4 RGPD).

Concrètement, c’est l’hypothèse d’un piratage de l’ordinateur d’un collaborateur, d’une faille des systèmes informatiques entraînant la disparition des données, d’un cambriolage de vos locaux professionnels entraînant le vol de vos dossiers ou même de la vente des contacts clients par un employé malveillant à un concurrent. Il peut également s’agir d’un employé malveillant qui vend les contacts clients à un concurrent.

- Cela peut aussi provenir de la nature même du traitement lorsque le traitement a pour objet des données sensibles.

Pour rappel, les données sensibles sont une catégorie de données listées à l’article 9 RGPD et pour lesquelles une protection renforcée est prévue. En principe tout traitement sur des données sensibles est interdit sauf exceptions (consentement, données publiques etc.).

Il s’agit d’informations relatives à l’origines raciale, ethnique, opinions politiques, religieuses, philosophiques, appartenance syndicale, données de santés (y compris numéro de sécurité social ou NIR), données biométriques et génétiques.

Il existe une autre catégorie de données perçues comme sensibles : les informations relatives aux condamnations pénales et infractions d’une personne (article 10 RGPD), les données de géolocalisation et les données bancaires.

Ces données comportent en elles-mêmes un risque élevé pour la vie privée des personnes.

- Le risque peut également avoir comme source la catégorie de personnes concernées par le traitement.

En effet, le RGPD accorde une protection particulière aux données personnelles de personnes vulnérables. C’est le cas des personnes mineures, et en particulier de moins de 15 ans (considérant 75 RGPD), demandeurs d’asile, de patients, de personnes âgées ou encore d’un employé dans les rapports avec son employeur. Ici c’est le déséquilibre entre le propriétaire de la donnée et son destinataire qui justifie qu’il existe un risque plus élevé.

- Enfin, le risque pour les droits et libertés des personnes peut provenir de l’utilisation même des données ou de la technologie utilisée.

Par exemple, le RGPD accorde une attention particulière aux décisions automatisées ou profilage. Ce sont des traitements dans lesquels un algorithme est utilisé pour évaluer certains aspects comportementaux d'une personne (article 22 RGPD).

Par exemple, un établissement bancaire utilise un algorithme qui se fonde sur tout un tas de critères pour déterminer le taux d'emprunt et donc d'accès au crédit. Un système similaire est utilisé par les sites de la grande distribution : votre comportement d'achat est analysé pour vous proposer des produits en particulier. C'est également le même système sur les réseaux sociaux où l'algorithme vous propose certains contenus en fonction de votre comportement.

En définitive, que la source du risque soit liée à sa nature, son utilisation, sa sécurité ou à la catégorie de personnes concernées, un risque élevé entraîne l'obligation de mener une analyse d'impact.
Dans un tel cas, l'article 35 RGPD impose au responsable de traitement de mener une analyse d'impact avant la mise en œuvre du traitement.

Votre entreprise procède à de nombreux traitements très différents. L'analyse d'impact peut concerner qu'un seul de ces traitements (un seul fichier ou une seule utilisation).

Par exemple, si 1% de vos utilisateurs sont mineurs, un PIA peut s'imposer à propos de ce nombre réduit de traitement.

ll est tout à fait possible qu'au jour du lancement de votre activité, vos traitements de données personnelles ne nécessitent pas de PIA.

Mais au cours de l'évolution de votre activité, vos traitements peuvent concerner des catégories différentes de personnes ou de données, ou la technologie utilisée devient plus sophistiquée.

Ainsi, un PIA peut s'avérer nécessaire après le lancement de votre traitement si bien qu'il est nécessaire de constamment s'interroger sur les risques.

Afin de guider les acteurs dans la mise en œuvre de leur conformité, le Groupe 29 (groupe de travail institué par l'article 29 de la directive européenne 95/46/CE), a publié des lignes directrices. Ce document décrit un certain nombre de critères permettant d'évaluer le niveau de risque.

3. DEVEZ-VOUS RÉALISER UN PIA ?

Votre traitement de données personnelles engendre-t-il un risque pour la vie privée des personnes ?

AVEZ-VOUS L'OBLIGATION DE RÉALISER UN PIA ?

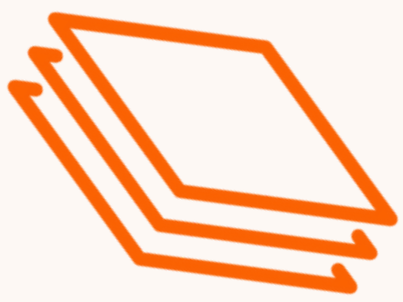
Par une lecture combinée de l'article 35 RGPD et des lignes directrices du Groupe 29, la CNIL a établi une **liste de questions à se poser dans un ordre précis afin de déterminer si un PIA est obligatoire.**

Pour résumer :

- Question n°1 : mon traitement est-il dans la liste des traitements pour lesquels **un PIA n'est pas obligatoire** ?
  - Si oui, pas d'obligation de réaliser un PIA. ✔
  - Si non, question n°2. ✖

- Question n°2 : mon traitement est-il dans la liste des traitements pour lesquels **un PIA est obligatoire** ?
  - Si oui, PIA. ✔
  - Si non, question n°3. ✖

- Question n°3 : mon traitement remplit-il **deux des neuf critères** ?
  - Si oui, PIA. ✔
  - Si non, pas d'obligation de réaliser un PIA. ✖



Dans les hypothèses où un PIA n’est pas obligatoire, cela ne signifie pas que vous ne devez pas en faire un. En toutes hypothèses, vous êtes responsable de l’analyse du risque de votre traitement.

Ces critères ne sont que des indices pour évaluer le degré de risque. Le fait que votre traitement ne corresponde à aucun de ces critères ne signifie pas qu’il n’existe aucun risque pour les droits et libertés des personnes. C’est à vous d’en juger.

Notre conseil : même si votre traitement correspond à un critère pour lequel un PIA n’est pas obligatoire, continuez la lecture de ce guide car l’obligation de réaliser un PIA pourrait concerner un traitement auquel vous n’avez peut être pas pensé.

Voyons ensemble plus en détails la liste de ces traitements et de ces critères : traitements pour lesquels un PIA n’est pas obligatoire (étape n°1), traitements pour lesquels un PIA est obligatoire (étape n°2) et liste des critères pour lesquels un PIA est obligatoire (étape n°3).

Étape n°1 - Traitements pour lesquels un PIA n’est pas obligatoire

Lorsque le traitement est très similaire à un traitement ayant déjà fait l’objet d’un PIA.

Bien que ce premier critère paraisse évident, il convient de préciser ce qu’il faut entendre par “similaire”.

Par exemple :
Une entreprise disposant de plusieurs lieux de travail (par exemple un siège à Paris, Lyon et Marseille) pour ses employés, souhaite installer un dispositif de caméra de surveillance à l’intérieur des locaux. Le siège à Paris peut tout à fait réaliser un seul PIA sur le dispositif de vidéosurveillance qui sera ensuite déployé dans les différents bureaux.

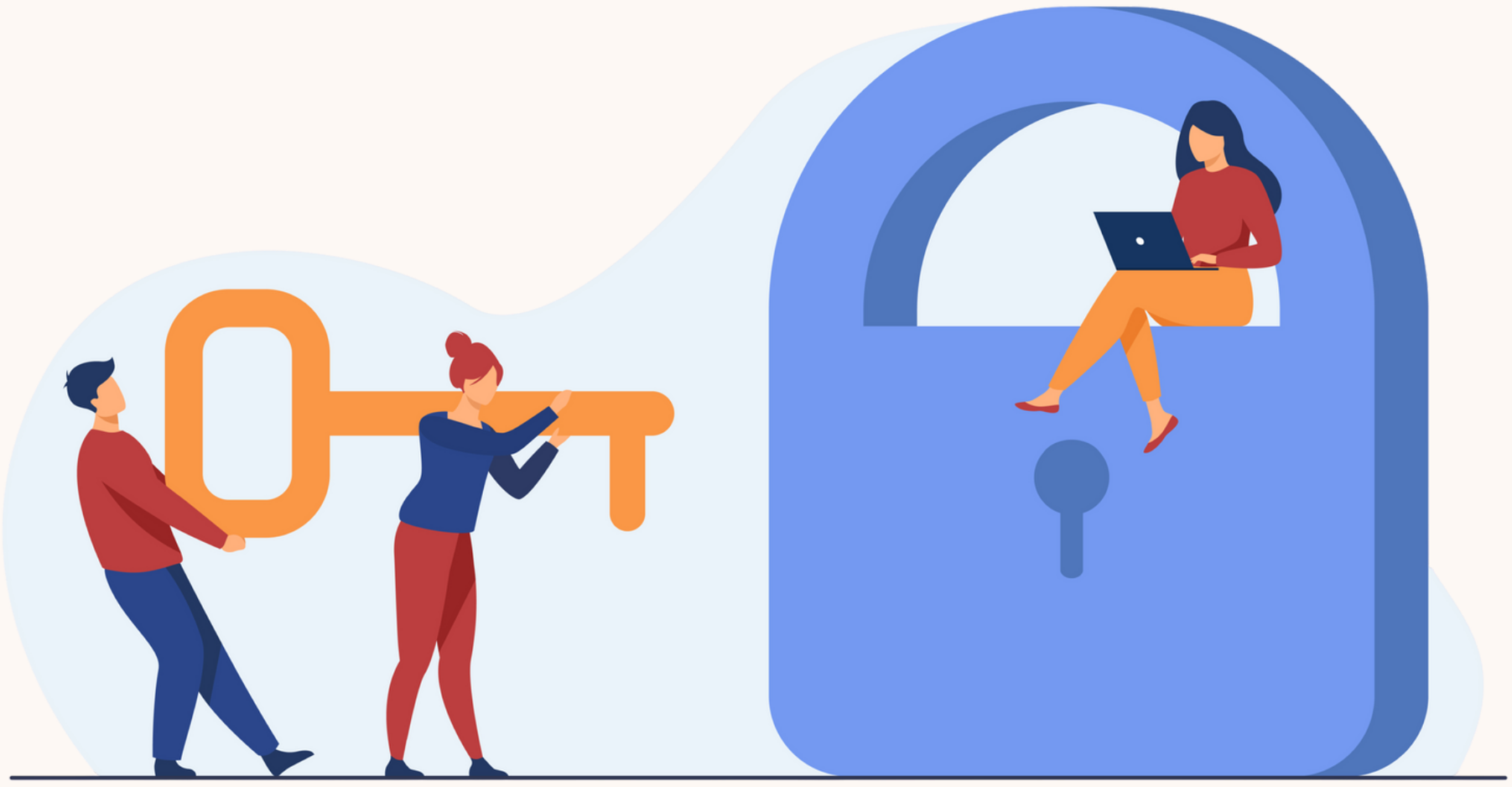
Lorsque le traitement est dicté par une obligation légale ou lorsqu’il est nécessaire à l’exercice d’une mission de service public et s’il rempli les deux conditions suivantes :

- Le droit réglemente cette opération de traitement. C'est-à-dire que le traitement est prévu par la loi au sein de laquelle sont également prévues des garanties pour les personnes concernées,
- Un PIA a déjà été mené pour l’adoption de cette loi. Il est assez courant qu’au cours de l’adoption de la loi, une étude d’impact soit réalisée. Donc a priori, il n’est pas nécessaire d’en refaire une.

Pour mieux comprendre ce critère il convient de rappeler certains éléments.

Un responsable de traitement peut valablement collecter et utiliser des données personnelles dans 6 cas, aussi appelés “bases légales” ce qui correspond au fondement juridique autorisant la collecte des données personnelles (article 6 RGPD) :

- La personne donne son consentement,
- Le responsable de traitement doit traiter ces données pour l’exécution d’un contrat,
- Le responsable de traitement estime qu’il a un intérêt légitime,
- Le responsable de traitement doit traiter ces données en vertu d’une obligation légale,
- Le responsable de traitement doit traiter ces données pour l’exécution d’une mission de service public,
- Le responsable de traitement doit traiter ces données pour la sauvegarde d’un intérêt vitale.



Si l’on reprend notre critère, il signifie que lorsque le responsable de traitement collecte des données fondées sur une obligation légale ou l’exercice d’une mission de service public, il convient de vérifier si la loi prévoyant ce traitement réglemente cette opération (1) et a été accompagnée d’une analyse d’impact (2). Dans cette hypothèse, un PIA n’est donc pas nécessaire.

Par exemple :
La loi prévoit que les employeurs doivent délivrer des bulletins de salaire à ses employés (qui contiennent des données personnelles) - la base légale est l’obligation légale.

La loi prévoit que les établissements scolaires sont chargés d’une mission de service public relative à l’éducation. Ils ont l’obligation à ce titre de collecter des données relatives aux notes des élèves, absences, retards, dossiers disciplinaires etc. - la base légale est l’exercice d’une mission de service public.

Dans ces cas (obligation légale et service public), le responsable de traitement doit vérifier si la loi réglemente l’opération de traitement et si une analyse d’impact a d’ores et déjà été menée pour l’adoption de la loi. Si tel est le cas, un PIA n’est pas nécessaire.

Dans des organismes qui emploient moins de 250 personnes et lorsque le traitement est mis en œuvre pour la seule gestion du personnel.

Il s'agit des traitements qui sont opérés à des fins de ressources humaines : gestion de la paie, formation, note de frais, outils de communication du personnel, évaluations du personnel, tickets restaurants etc. Pour ces traitements, un PIA n'est pas nécessaire car ils n'engendrent que peu de risque pour les droits et libertés des personnes concernées.

Dès lors que le traitement prévoit la collecte de données sensibles ou un profilage, le traitement n'entre plus dans cette catégorie et il convient d'étudier le reste des critères.

Par exemple :

Si un fichier RH prévoit un système d'avancement de carrière selon l'appartenance à un syndicat, c'est une donnée sensible (par ailleurs, ce n'est tout simplement pas un traitement autorisé puisque la RATP s'est faite sanctionnée par la CNIL à hauteur de 400.000 euros).

Lorsqu'un algorithme permet d'automatiser l'avancement de carrière des employés en analysant plusieurs données relatives à leur comportement dans l'entreprise. Il s'agit de profilage (article 22 RGPD).

Ces hypothèses sont exclues de ce critère.

Lorsque le traitement est relatif à la relation fournisseurs.

Il s’agit des traitements liés aux tâches administratives pour l’exécution d’un contrat ou d’un futur contrat avec un fournisseur : commandes, factures, comptabilité, ordre de paiement, statistiques fournisseurs, documentation fournisseurs etc.

Ces traitements ne contiennent en eux-mêmes aucun risque pour les droits et libertés des personnes.

Lorsque le traitement est relatif à la gestion du fichier électoral des communes.

Ce critère est très spécifique aux collectivités territoriales, qui par nature, sont amenées à opérer un certain nombre de traitements similaires.

Dans la mesure où le fichier électoral ne contient naturellement pas de données sur l’opinion politique des administrés (nom, prénom, adresse, bureau de vote), il n’engendre aucun risque et n’entraîne pas la réalisation d’un PIA.

Lorsque le traitement est relatif à la gestion des activités des comités d'entreprises.

Comme pour le critère précédent, il s'agit d'un traitement assez générique et dont on sait qu'il ne conduit pas à engendrer un risque élevé pour la vie privée des employés.

Lorsque le traitement est relatif à la gestion des membres et des donateurs des associations, fondation et organisme à but non lucratif.

Ce traitement assez classique pour les associations, organisme à but non lucratif, partis politiques, ONG etc.

Cependant, il convient de préciser qu'il est uniquement question de la gestion interne des membres : gestion des évènements, communication interne et externe, élection des membres, gestion des réunions etc.

En dehors de ces hypothèses, il convient d'analyser le risque lié au traitement, en particulier lorsque les membres sont amenés à communiquer des opinions politiques, religieuses, philosophiques ou des données de santé (données sensibles).

Lorsque le traitement est nécessaire à la prise en charge d’un patient par un professionnel de santé.

Ce critère concerne les traitements qui sont opérés par un médecin exerçant dans un cabinet médical ou un laboratoire médical ou un pharmacien dans une officine à propos de données sur la prise de rendez-vous et le dossier médical du patient.

Alors même qu’il s’agit de données sensibles (données de santé) concernant des personnes vulnérables au sens du RGPD (patients) le traitement ne nécessite pas de PIA car il est opéré par un professionnel de santé soumis au secret médical.

Nous verrons plus bas que pour le traitement de données personnelles de patients par les hôpitaux s’agissant de leurs rendez-vous et dossier médical, ces établissements ont l’obligation de réaliser un PIA. En effet, ici s’ajoute un élément à risque lié au nombre de personnes et de données en jeux.

Lorsque le traitement est mis en œuvre par un avocat ou un notaire dans l'exercice de sa profession.

Comme pour les médecins, les avocats, notaires et huissiers sont des professions réglementées soumises au secret professionnel.

Pour cette raison, les traitements, y compris concernant de données sensibles sur des personnes vulnérables (mineurs, patients, demandeurs d'asiles, travailleurs etc.), sont protégés par le secret et ne nécessitent pas de PIA.

Lorsque le traitement est mis en œuvre par les collectivités territoriales, personnes morales de droit public et privé pour la gestion des services publics scolaire, périscolaires et petite enfance.

Ce critère est très spécifique au secteur de la petite enfance et aux activités périscolaires prises en charge par des personnes publiques ou des personnes privées. Au regard du peu d'informations à risque collectées pour l'exercice de cette activité, un PIA n'est pas nécessaire.

Lorsque le traitement est mis en œuvre aux seules fins de gestion des contrôles d’accès physiques et horaires pour le calcul du temps de travail.

Ce critère recouvre deux hypothèses :

1. Un dispositif d’accès au lieu de travail, par exemple par un badge. Ce traitement ne nécessite pas de PIA s’il ne contient pas de données biométriques (scan du visage, de la main, ou de n’importe quelle particularité physique permettant d’identifier spécifiquement une personne via une technologie).
    - Par exemple, il arrive que certains dispositifs d’accès au lieu de travail prévoient un scan de la taille de la main pour accéder au lieu de travail. Ce sont des données biométriques et donc sensibles exclues de ce critère.
2. Un dispositif de contrôle du temps de travail uniquement si la finalité est la gestion du temps de travail.
    - Par exemple, si un dispositif qui prévoit la surveillance accrue des employés n’entre pas dans cette catégorie.

Si votre traitement est concerné par l’un de ces 11 critères, il n’est pas obligatoire de procéder à une analyse d’impact.

En tout état de cause, le RGPD vous laisse seul décideur, en dépit de ces critères. Vous êtes responsable de la décision de réaliser un PIA, ou pas.

Étape n°2 - Traitements pour lesquels un PIA est obligatoire

Il s’agit des traitements qui engendrent en eux-mêmes un risque élevé pour les droits et libertés des personnes concernées.

Cette liste de traitement n’est pas exhaustive. D’autres traitements en dehors de cette liste peuvent engendrer un risque élevé pour la vie privée des personnes (c’est toute la difficulté).

Pour cette raison, la CNIL a établi une seconde liste pour couvrir un champ plus large d’hypothèses.

Méthode d’analyse : Si votre traitement est concerné par la première liste (étape n°2), un PIA est obligatoire. Sinon, il convient de se référer aux critères de la seconde liste (option n°2), si votre traitement concerne au minimum deux critères, un PIA s’impose.

Option n°1 - Traitements entraînant l’obligation de réaliser un PIA.

Lorsque le traitement est mis en œuvre par les établissements de santé concernant la prise en charge des personnes.

À la différence des médecins exerçant à titre individuel, les traitements de santé mis en œuvre par les hôpitaux, CHU, cliniques nécessitent un PIA. En effet, ces traitements s’opèrent sur des données sensibles, à propos de personnes vulnérables (patients) et à large échelle.
Les centres communaux d’action sociale (CCAS) et les EPHAD sont également concernés.

Lorsque le traitement est mis en œuvre pour un registre de données de santé.

Ce critère concerne tout type d’établissement, y compris une personne privée, opérant des traitements sur des registres de données de santé. Le traitement concerne des données de santé (sensibles) sur des personnes vulnérables (patients) à grande échelle.

Lorsque le traitement porte sur des données génétiques de personnes vulnérables.

Cette hypothèse renvoie aux traitements sur des données génétiques opérés par des établissements publics ou privés, notamment pour des activités de recherche médicale. Ici le risque est élevé en raison des traitements opérés sur des personnes vulnérables (patients), concernant des données sensibles (données génétiques) à large échelle.
Par exemple, Health Data Hub est un établissement procédant à ce type de traitement.

Lorsque le traitement établit des profils de personnes à des fins de gestion des ressources humaines.

Souvenez-vous, pour les organismes de moins de 250 personnes, lorsque le traitement est mis en œuvre pour la seule gestion du personnel, un PIA n’est pas obligatoire, sauf lorsqu’il a pour but d’opérer un profilage.

Pour rappel, un profilage ou décision automatisée est un traitement pour lequel un algorithme est utilisé pour évaluer certains aspects comportementaux d'une personne (article 22 RGPD).

Tel est le cas lorsque le traitement prévoit une évaluation des employés pour détecter les "hauts potentiels" ou lorsqu'un algorithme est utilisé pour l'avancée de carrière ou le recrutement. Ce système algorithmique peut conduire à priver les personnes d'un bénéfice (carrière, emploi, rémunération, formation etc.) sans intervention humaine. De plus il porte sur des personnes vulnérables : un employé dans ses rapports avec son employeur.

Dès lors, le risque porté aux personnes concernées est élevé et nécessite un PIA.

Lorsque le traitement a pour finalité de surveiller de manière constante l'activité des employés (cybersurveillance, vidéosurveillance etc.).

Les dispositifs de vidéosurveillance sur le lieu de travail ou de cybersurveillance sont de plus en plus courants.

Que ces contrôles s'opèrent sur vidéo ou sur internet, ils sont particulièrement intrusifs pour les employés dont le respect au droit à la vie privée ne s'arrête pas aux portes sur lieux de travail.

Dès lors que ce dispositif est particulièrement intrusif et mis en place sur des personnes vulnérables (travailleurs), un PIA s'impose.

Pour rappel, ces dispositifs doivent être mis en place dans des conditions particulières : une information complète et accessible doit être mise à disposition des personnes concernées.

Lorsque le traitement a pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire.

Ce type de traitement est très spécifique à la situation de la crise sanitaire et couvre tous les systèmes informatiques mis en œuvre par l'Etat pour la gestion de la crise sanitaire.

Lorsque le traitement a pour finalité la gestion des alertes et des signalements en matière professionnelle.

Ce type de traitement est également spécifique aux dispositifs de trafic d'influence ou de corruption au sein d'un organisme. Ces dispositifs sont également intrusifs dans la vie des personnes concernées.

Lorsque le traitement, par rapprochement de données ou par profilage, est susceptible d'exclure des personnes du bénéfice d'un contrat.

Le profilage ne conduit pas automatiquement à exclure les personnes d'un avantage ou d'un bénéfice mais lorsque tel est le cas, le risque est élevé.

Par exemple, il arrive que les établissements bancaires utilisent des algorithmes entièrement automatisés qui analysent des données personnelles pour calculer le taux d'emprunt accordé à un individu. Un taux très élevé conduit à exclure une personne du bénéfice d'un emprunt intéressant, sans intervention humaine. Le risque pour les droits et libertés des personnes est donc élevé.

D'ailleurs ce critère concerne également un simple rapprochement de données en dehors de tout profilage mais conduisant à exclure une personne de l'obtention d'un bénéfice d'un contrat (contrat de travail, contrat de vente, etc.).

Lorsque le traitement réalise un profilage à l'aide de données externes à l'organisme.

Nous l'avons vu, le profilage comporte des risques pour les individus. Il est d'autant plus grand lorsque les personnes concernées ne sont pas informées du traitement opéré. C'est le cas lorsque le profilage est réalisé à l'aide d'un rapprochement de données achetées auprès de courtiers de données par exemple. Par exemple pour de la publicité en ligne.

Lorsque le traitement concerne des données biométriques de personnes vulnérables.

Comme précédemment vu, les traitements concernant des données sensibles, telles que les données biométriques, sur des personnes vulnérables (mineurs, patients, personnes âges etc.) engendrent un risque important.

Par exemple, un certain nombre d'établissements scolaires ont mis en place un contrôle d'accès des cantines aux élèves (mineurs) par un système de reconnaissance du contour de la main (données biométriques). L'ensemble de ces établissements ont été tenus, préalablement au traitement, de réaliser un PIA.

Lorsque le traitement concerne des données de localisation à large échelle.

Bien que les données de géolocalisation ne soient pas définies comme des données sensibles au sens de l'article 9, ces données sont considérées "comme sensibles" par la CNIL.

En effet, ces données comportent en elle-même un risque élevé pour la vie privée des personnes en cas de divulgation ou fuite non autorisée. Le risque est d'autant plus élevé lorsque ces données sont collectées à large échelle ce qui justifie la réalisation d'un PIA.

Par exemple, les applications comme Waze et Google Maps seraient potentiellement concernées.

Lorsque le traitement concerne la gestion des logements sociaux ou l'accompagnement médico-social ou social.

Ce critère est assez spécifique à un secteur donné : logements sociaux, établissements de réinsertion sociale et professionnelle, personnes handicapées etc. Le traitement porte par nature sur des données sensibles de personnes vulnérables.

S'il est vrai que cette liste est longue, la plupart d'entre elles concernent des secteurs spécifiques d'activités.

Or, en dehors de ces secteurs d'activités, les traitements opérés par les entreprises peuvent également comporter des risques pour la vie privée des personnes.

Les 9 critères établis par la CNIL sur le fondement des lignes directrices du Groupe 29 permettent d'éclairer les acteurs sur l'appréciation du degré de risque. Si le traitement envisagé concerne au minimum deux d'entre eux, alors un PIA est obligatoire.

Étape n°3 - Critères entraînant l’obligation de réaliser un PIA.

C’est la dernière étape de la démarche (promis !) :

- Si votre traitement ne se trouve pas dans la liste de ceux pour lesquels un PIA n’est pas obligatoire (étape n°1),
- Ni ne se trouve dans la liste des traitements pour lesquels un PIA est obligatoire (étape n°2),
- Il convient de vérifier si le traitement concerne au minimum deux des neuf critères suivants. Si tel est le cas, un PIA s’impose.

1. **Toute opération de traitement consistant en une évaluation, notation, profilage ou prédiction.**

Comme vu précédemment, le profilage ou les systèmes d’analyse de comportement pour attribuer une notation ou un avantage comportent un risque important pour la vie privée des personnes.
Par exemple, un fichier RH consistant à évaluer le comportement des employés pour leur avancement de carrière.

2. Toute opération de traitement par décision automatique avec effet légal ou similaire.

Le risque est encore plus élevé lorsque le profilage conduit à exclure une personne du bénéfice d’un contrat ou d'un avantage.

Par exemple, c’est le cas des systèmes algorithmiques des établissements bancaires pour évaluer l’accès d’une personne à un crédit bancaire.

3. Toute opération de surveillance systématique.

Tout système de surveillance comporte par nature un risque pour la vie privée des individus.

C’est le cas des systèmes de cybersurveillance ou de vidéo surveillance des employés sur leur lieu de travail. C’est également le cas de la vidéo surveillance dans l’espace public.

4. Toute opération de traitement visant à la collecte de données sensibles ou à caractère hautement personnel.

Les données sensibles sont les informations relatives à l'origine raciale, ethnique, opinions politiques, religieuses, philosophiques, appartenance syndicale, données de santés, données biométriques et génétiques (article 9 RGPD).

Les données à caractère hautement personnel sont relatives aux condamnations pénales et infractions d'une personne (article 10 RGPD).

Précisons également que la CNIL considère les données bancaires sont "perçues comme sensibles" et leur accorde le même niveau de protection.

De la donnée sensible peut se cacher dans beaucoup de données qui, a priori, n’en contiennent pas.

Par exemple :

- La photo ou le nom d’un candidat à un emploi, peuvent contenir des informations sur ses origines ethniques et raciales que l’employeur traite lors de la procédure de recrutement.
- L’achat d’un livre religieux est une information relative aux convictions religieuses qu’un site de e-commerce peut être amené à traiter.
- Les données de santé correspondent une catégorie particulièrement large : numéro de sécurité sociale (NIR), identité du médecin en charge de cette personne, type de traitement pris, état de santé passé, présent et futur etc.

Pour savoir si votre structure traite de la donnée sensible, tout dépend du contexte.

Le Groupe 29, dans son rapport, explique que le traitement de données sensibles dépend “non pas du contenu des données elles-mêmes mais du contexte dans lequel elles sont utilisées” à l’exception de “certaines catégories de données peut, en tant que tel, porter préjudice aux droits et intérêts des individus”.

Les catégories de données considérées comme sensibles en tant que telles sont les données biométriques, génétiques et certaines données de santé qui comportent un risque pour la vie privée en elles-mêmes. Pour ces données, seules les exceptions prévues à l’article 9 RGPD permettent leur traitement.

Pour le reste, c’est la finalité du traitement qui va être déterminant pour la qualification de donnée sensible et le contexte du traitement.

Au regard de ces éléments, votre entreprise peut être amenée à traiter de la donnée sensible : numéro de sécurité social de vos employés ou données bancaires de vos clients. Il convient d’être vigilant à l’égard de ces données.

5. Toute opération de traitement visant à la collecte de données personnelles à large échelle.

Ici c’est le nombre très important de données ou de personnes concernées par le traitement qui est porteur d’un risque.

Pour déterminer ce qu’est un traitement “à large échelle”, le Groupe 29 recommande de prendre en compte les éléments suivants :

- Le nombre important de données ou de personnes concernées,
- La catégorie de données traitées (données sensibles, hautement personnel, données de géolocalisation etc.),
- La permanence de l’activité (par exemple la géolocalisation constante), Et l’étendue géographique des activités.

Par exemple, sont des traitements opérés à large échelle les traitements suivants :

- Les traitements de données de patients par un hôpital,
- Les traitements de données de clients d'une banque ou d'une compagnie d'assurance,
- Les traitements opérés par une collectivité territoriale,
- Les traitements de données de personnes sur un moteur de recherche, Les traitements de données de géolocalisation d'une application mobile.

À l'inverse, un médecin ou un avocat exerçant à titre individuel n'effectue pas de traitement à large échelle.

6. Toute opération visant à croiser deux opérations de traitements collectées à des fins différentes ou par des responsables de traitement différents d'une manière outrepassant les attentes raisonnables des personnes concernées.

Ce critère décrit les hypothèses dans lesquelles un organisme achète des bases de données, ou utilise des données accessibles publiquement à d'autres fins pour opérer un croisement de données.

7. Toute opération de traitements relatifs à des personnes vulnérables.

La liste des personnes considérées comme vulnérables au sens du RGPD n’est pas définie de manière exhaustive.

Ce qui est sur, c’est qu’il s’agit des personnes mineures, en particulier les mineurs de moins de 15 ans, les personnes âgées, les patients, les employés dans leurs rapports avec leurs employeurs, ainsi que les demandeurs d’asiles, personnes souffrant de maladie mentale ou vulnérables en raison de leurs situations particulières.

Leurs données sont mieux protégées en raison de la difficulté pour eux d’exprimer librement leur consentement aux traitements de leurs données ou de s’opposer à un tel traitement.

8. Usage d’une technologie innovante ou utilisation d’une nouvelle technologie.

Ce critère est justifié par le fait que l’usage d’une nouvelle technologie peut impliquer de nouvelles formes de traitement des données personnelles. Par exemple l’utilisation d’une nouvelle intelligence artificielle.

9. Toute opération de traitements qui en eux-mêmes conduisent à exclure une personne du bénéfice d'un droit ou d'un contrat.

Il s'agit de tous types d'opération de traitement qui, sans utiliser un système algorithmique, profilage ou décision automatisée, conduit à exclure un individu du bénéfice d'un droit ou d'un service.

Par exemple, un traitement de données personnelles qui conduit à exclure une personne un réseau social ou un crédit bancaire non accordé à un individu suite à l'analyse de ses données (sans algorithme).

En définitive, plus le traitement remplit de critère plus il engendre un risque pour les droits et libertés des personnes. À partir de deux critères, un PIA est obligatoire.

Exemples d’application de ces critères :

Exemple n°1 : lorsqu’un employeur met en place un système de surveillance de ses employés par un système vidéo dans les locaux de l’entreprise ou un système de surveillance de leurs activités sur internet, le traitement correspond à une surveillance systématique (critère n°3) et de personnes vulnérables (critère n°7).

Exemple n°2 : lorsque des entreprises collectent des données personnelles publiques sur les réseaux sociaux, dans le but de générer des profils. Le traitement correspond à des données traitées à grande échelle (critère n°5) sensibles (critère n°4) par un croisement ou une combinaison d’ensemble de données (critère n°6).

Exemple n°3 : à l’inverse, un média en ligne qui utilise la liste de contacts de ses abonnés pour les informer par email de la parution d’un nouveau numéro est un traitement opéré à large échelle (critère n°5) mais aucun autre critère n’est rempli. Un PIA n’est pas nécessaire.

Exemple n°4 : le 10 novembre 2022, la CNIL a prononcé une sanction à l'encontre de la société DISCORD INC pour son manquement à l'obligation d'effectuer une analyse d'impact. La société DISCORD permet à des utilisateurs de jeux vidéo de communiquer via leur microphne, webcam ou messagerie instantanné. La CNIL a considéré que deux critères étaient remplis : l'entreprise traite des données de personnes vulnérables (moins de 18 ans)(critère n°7) et à large échelle aux vues du nombre de personne (critère n°5). Dès lors l'entreprise était tenue de réaliser un PIA.

La CNIL l'a rappelé à plusieurs reprises, le fait que votre traitement ne concerne qu'un seul de ces critères peut néanmoins être susceptible d'engendrer un risque pour les droits et libertés des personnes. Vous êtes seul responsable de l'appréciation de ce risque.

En tout état de cause, il ne faut pas envisager le PIA comme une contrainte mais bien comme une formidable opportunité de démontrer votre sérieux à vos équipes, vos clients et vos partenaires.

Il est un outil puissant pour vous démarquer de la concurrence.

4. COMMENT RÉALISER UN PIA

Analysez le risque et établissez un plan d’action pour le réduire.

COMMENT RÉALISER UN PIA ?

Si votre traitement engendre un risque élevé pour les droits et libertés des personnes, vous avez l'obligation de réaliser un PIA. La CNIL a déjà eu l'occasion de sanctionner **plusieurs entreprises n'ayant pas suffisamment apprécié la gravité du risque.**

Si vous êtes effectivement concerné par l'obligation de réaliser un PIA, plusieurs questions doivent vous interpeller dans cet ordre :

- Quand réaliser son PIA ?
- Quels sont les acteurs impliqués dans la réalisation du PIA ?
- Quelle est la méthode pour réaliser un PIA ?
- Faut-il consulter la CNIL au préalable ?
- Enfin, faut-il publier son PIA ?

Quand réaliser son PIA ?

En principe, le PIA doit être réalisé avant le traitement envisagé (article 35 RGPD).

Cette exigence rejoint un autre principe important du RGPD, celui du “Privacy by Design” qui signifie que le responsable de traitement doit garantir un niveau approprié de sécurité dès la conception du traitement de données personnelles (article 25 RGPD).

Le PIA est conçu comme un outil permettant de décider comment le traitement doit être opéré et aider le responsable de traitement à savoir s’il est en mesure de garantir le niveau de sécurité suffisant pour le traitement de données personnelles qu’il envisage.

Pas d’inquiétude si vous n’avez pas effectué votre PIA avant votre traitement. L’analyse d’impact est avant tout un processus sur la durée. Au cours de l’évolution de votre activité vous devez continuellement vous interroger sur la nécessité de réaliser une analyse d’impact.

Ainsi, un traitement qui ne nécessitait pas d’analyse d’impact lors de sa conception peut progressivement en nécessiter une si la technologie utilisée évolue, si les catégories de données ou de personnes concernées changent etc.

De plus, à partir du moment où vous avez réalisé un PIA, il convient de le mettre à jour au regard des évolutions de votre traitement. Il est assez courant que les entreprises revoient les éléments de sécurité prévus dans l’analyse d’impacttous les 2/3 ans.

C’est donc au moment où vous considérez qu’il existe un risque pour la vie privée des personnes concernées qu’il est opportun d’effectuer un PIA.

Quels sont les acteurs impliqués dans la réalisation du PIA ?

Il existe plusieurs acteurs clés dans la réalisation du PIA :

- Le responsable de traitement,
- Le délégué à la protection des données (DPO),
- Les sous-traitants,
- Les personnes concernées,
- Vos collaborateurs.

Rôle du responsable de traitement dans le PIA.

L’article 35 RGPD est clair sur ce point : la responsabilité de veiller à ce que soit réalisé un PIA incombe au responsable de traitement. Il est également seul responsable de la décision de ne pas en réaliser un.

Si la responsabilité lui incombe, il n’est pas chargé de sa réalisation. Le PIA peut être réalisé par la société mère pour le compte de sa filiale, par un cabinet d’audit externe, par le délégué à la protection des données personnelles (DPO) en interne.

Devez vous faire un PIA lorsque vous avez le statut de sous-traitant ? Non.

La CNIL est claire sur ce point “Votre client, en tant que responsable de traitement, doit réaliser une analyse d’impact des traitements envisagés sur la protection des données dans les conditions prévues à l’article 35 du règlement européen. La réalisation d’une telle analyse ne relève donc pas de votre responsabilité.”

Il aurait été sûrement plus simple pour le sous-traitant d’être chargé de réaliser une analyse d’impact par exemple sur la technologie qu’il met ensuite à disposition de ses clients afin de décharger ces derniers. Cet élément a notamment été débattu lors de l’adoption du RGPD qui prévoyait à l’origine une obligation de PIA pour les sous-traitants.

Il en a été jugé autrement car les sous-traitants ne traitent finalement des données personnelles que sur instructions des responsables de traitement qui eux, utilisent réellement ces données.

Si votre entreprise a le statut de sous-traitant pour certaines activités, vous avez la casquette de responsable concernant les traitements que vous effectuez pour votre compte : traitements RH, analyse statistique de vos clients, fichiers clients, etc.

Ces traitements peuvent faire l'objet d'un PIA dès lors que vous en êtes responsable.

En revanche, le sous-traitant doit apporter des garanties de sécurité des données qu'il traite pour le compte du responsable de traitement.

Ces garanties doivent faire l'objet d'un contrat souvent dénommé accord de traitement des données Data Processing Agreement (DPA).

Le contenu de ce contrat est fixé par l'article 28 RGPD (concernant les sous- traitants) :

- L'objet, la durée, la nature et la finalité du traitement et le type de données personnelles. Par exemple si les données présentent un caractère sensible,
- Les instructions du responsable de traitement, c'est-à-dire la manière dont il souhaite que les données soient utilisées,
- Les mesures techniques et organisationnelles prévues pour garantir la sécurité des données,
- Les conditions dans lesquelles le sous-traitant assiste le responsable de traitement, et notamment pour la réalisation du PIA.

Par exemple, lorsqu'une personne exerce son droit sur ses données personnelles en demandant la suppression intégrale de ses données, le contrat doit prévoir en combien de temps le sous-traitant répond à la demande du responsable de traitement pour supprimer une donnée ou s'il met à disposition un portail dédié.

- Le contrat doit prévoir en combien de temps le sous-traitant met à disposition du responsable de traitement toutes les informations dont il a besoin pour la réalisation de l’analyse d’impact.

- Le contrat doit également prévoir le nom de l’interlocuteur à contacter (équipe technique, DPO, CTO etc.), la nature des informations qui pourront être délivrées etc. (nous reviendrons sur ces éléments ci- dessous).

- Enfin, il peut contenir tout ou partie des clauses contractuelles types (CCT).

Ces clauses ont été adoptées par la Commission européenne et permettent d’assurer un minimum de conformité aux exigences du RGPD.

Ces clauses ont pour objet de vous aider à la rédaction d’un tel contrat.

Rôle du délégué à la protection des données (DPO) dans le PIA.

Le Groupe 29 a précisé dans ses lignes directrices le rôle du DPO dans la mise en œuvre du PIA.

Le délégué à la protection des données ou data protection officer (DPO) est la personne en charge de la protection des données au sein d'un organisme ou d'une entreprise. Il a naturellement le rôle d'assister le responsable de traitement dans la réalisation d'un PIA.

Sur demande du responsable de traitement, le DPO a l'obligation d'émettre des avis sur :

- La nécessité de faire un PIA, La méthode à utiliser,
- Les mesures de protection à adopter pour réduire les risques d'atteinte à la vie privée des personnes,
- Sur les conclusions du PIA et sa conformité au RGPD.

En effet, l'article 39 RGPD précise notamment que le DPO a la mission de "dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35".

Pour rappel, le responsable de traitement reste seul décideur. Il peut aller à l'encontre des recommandations du DPO mais doit dans ce cas le documenter et le justifier au sein du PIA ou d'un document à part.

Rôle des sous-traitants dans le PIA.

Comme vu plus haut, il ressort des article 35 RGPD (PIA) et article 28 RGPD (sous-traitants) que le sous-traitant doit assister le responsable de traitement dans la conduite du PIA et fournir toutes les informations nécessaires pour sa réalisation.

Les obligations précises du sous-traitant envers le responsable de traitement doivent être prévues dans le contrat établissant cette relation. Ce contrat doit notamment prévoir :

- Les conditions dans lesquelles le sous-traitant délivre toutes les informations nécessaires concernant le traitement en cause : qui est l'interlocuteur, en combien de temps le sous-traitant répond aux demandes d'assistance du responsable de traitement, sous quel format, etc.
- Le contenu des informations qui pourront être communiquées : la technologie utilisée pour le traitement de ces données, les mesures organisationnelles et techniques protégeant les données, la liste des personnes ayant accès à ces données, etc.
- Le degré d'assistance que le sous-traitant envisage de donner et si elle engendre un coût supplémentaire que le responsable de traitement devra financer.

Par exemple, les clauses contractuelles types (CCT) adoptées par la Commission européenne sont rédigées ainsi :

"Clause 8

Assistance au responsable du traitement

(...)

c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :

1) L'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel («analyse d'impact relative à la protection des données») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques.

2) L'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque".

Il est fortement recommandé de négocier des clauses beaucoup plus précises que le niveau de détail proposé par la clause 8. Vous pouvez les retrouver en détail ici.

Rôle des personnes concernées.

Le responsable de traitement sollicite, le cas échéant, l’avis des personnes concernées ou leurs représentants (article 35 RGPD). On entend par “personnes concernées” les personnes auxquelles appartiennent les données personnelles faisant l’objet du traitement pour lequel une analyse d’impact est réalisée.

La consultation des personnes concernées peut apporter une plus-value dans l’identification des risques dans le PIA. C’est également un vecteur de transparence et de réassurance des clients, partenaires et employés.

Par exemple, le responsable peut solliciter les représentants du personnel avec un questionnaire concernant la mise en place d’un système de vidéosurveillance sur le lieu de travail.

Sur la forme, précisons que recueillir le simple consentement des personnes concernées pour le traitement des données personnelles ne suffit pas pour recueillir leurs avis sur le PIA. En pratique, les avis des personnes concernées peuvent être recueillis par sondage, enquête, formulaire. La forme est relativement libre dès lors que le but est atteint.

Selon le G29, si le responsable de traitement prend une décision différente de l'avis formulé par les personnes concernées, il doit documenter de manière précise les raisons pour lesquelles il persiste dans le lancement du traitement contrairement aux avis formulés.

Toutefois, la décision de consulter ou non les personnes concernées revient au responsable de traitement. Il est possible pour ce dernier de ne pas recueillir les avis mais il doit en justifier toutes les raisons dans le PIA. Par exemple, si la confidentialité des affaires est en jeu. L'important est de documenter les raisons pour lesquelles cette consultation n'est pas souhaitable ou réalisable.

Rôle de vos collaborateurs.

Enfin, aidez-vous de vos collaborateurs ! En particulier les collaborateurs impliqués dans la réalisation du traitement que vous projetez et les responsables de la sécurité informatique de vos systèmes. Il peut s’avérer que le responsable de la sécurité des systèmes d’information (RSSI) occupe un rôle très important pour la réalisation du PIA.

Construire un PIA en collaboration avec les équipes concernées est le meilleur moyen d’impliquer tous vos collaborateurs dans la protection des données personnelles et prévenir toute violation de celles-ci.

Quelle méthode pour réaliser un PIA ?

Comme exposé plus haut, le RGPD n’impose aucun formalisme. Si la forme est libre, la RGPD impose un certain nombre d’exigences.

Au préalable, notons que la CNIL a créé un logiciel permettant la conduite d'un PIA. Cependant, cet outil est pensé pour un public relativement expert de la question.

Nous vous proposons une clé de lecture simple des étapes à suivre.

Le paragraphe 7 de l’article 35 RGPD dispose que le PIA doit, au minimum, contenir les éléments suivants :

- Une description des opérations de(s) traitement(s) envisagé(s),
- L’évaluation de la nécessité de(s) traitement(s) et les mesures de sécurité en l’état,
- L’évaluation des risques pour les droits et libertés des personnes concernées,
- Et enfin les mesures envisagées pour réduire ce risque.

En tout état de cause, il convient de rappeler qu'une étude d'impact est "un processus d'amélioration continue pour parvenir à une réduction des risques acceptables" selon les termes exacts de la CNIL.

Cela signifie deux choses :

- Le PIA doit être mis à jour de façon continue, en moyenne tous les deux ans, afin de suivre les évolutions du contexte du traitement et de l'efficacité des mesures,
- La conformité n'est pas une fin mais un moyen. L'esprit est d'essayer d'arriver à réduire le risque au maximum.

Étape n°1 - Description des opérations de traitement envisagés.

La première marche du processus consiste à décrire tous les éléments de contexte du traitement à risque :

- Nature du traitement, ses finalités et ses enjeux,
- Identités du responsable de traitement, du DPO, de tous les sous-traitants impliqués,
- Catégories de personnelles concernées, leur durée de rétention des données, les propriétaires des données (par exemple si les données appartiennent à des personnes vulnérables).

Par exemple, une entreprise collectant des données de localisation de ses utilisateurs à travers une application mobile.

Il convient d'indiquer :

- L'objectif de la collecte de ces données,
- Le contexte dans lequel elles sont collectées,
- Comment elles sont collectées,
- Comment elles sont utilisées,
- Combien de temps elles sont conservées,
- Comment ces informations sont stockées,
- Les utilisateurs sont-ils bien informés de la collecte de ces données et de la possibilité d'exercer leurs droits, etc.

Étape n°2 - Evaluer la nécessité du traitement et du respect des droits des personnes concernées.

Cette deuxième partie se décompose en deux actions :

- L'évaluation de la nécessité du traitement,
- L'évaluation du respect des droits des personnes concernées.

Évaluation de la nécessité du traitement

L’article 35 RGPD prévoit que le responsable de traitement doit réaliser une évaluation de la nécessité et de la proportionnalité du traitement au regard de sa finalité. L’idée ici est de s’interroger plus largement sur la légalité du traitement.

In fine, cette étape doit permettre d’évaluer le rapport entre la nécessité de collecter une donnée personnelle et l’objectif pour lequel elle est collectée afin d’opérer une balance entre l’intérêt du responsable de traitement à collecter une donnée et l’intérêt de la personne concernée de la protéger.

Pour ce faire, les éléments suivants doivent être détaillés et justifiés :

- Finalité du traitement
  - C’est l’objectif pour lequel vous avez décidé de collecter ces données.
  - Par exemple, vous collectez des données “cookies” (adresse IP, identité de l’utilisateur, comportement sur la navigation, nombre de clics,appareil utilisé etc.). La finalité pourrait correspondre à l’établissement de statistiques sur le parcours client.

- Base légale du traitement
    - Il existe 6 bases légales : le consentement, l'obligation légale, l'exécution d'un contrat, l'intérêt légitime, l'intérêt public et la sauvegarde d'un intérêt vital (article 6 RGPD). C'est ce qui vous autorise à traiter ces données.
- Justification de l'étendue de la collecte des données
    - Cet élément est la traduction du principe de minimisation des données, selon lequel ne sont collectées que les données personnelles nécessaires au traitement et pas plus (article 5 RGPD). C'est l'élément le plus important de cette partie : justifier la nécessité du traitement au regard de la finalité.
    - Par exemple, une entreprise qui vend des rames de papier pour imprimantes. Une telle activité ne nécessite pas, a priori, de collecter les données biométriques pour accéder au lieu de travail car le produit vendu ne nécessite pas de telles mesures de sécurité. L'organisme n'est, a priori, pas légitime à collecter des données sensibles sur des personnes vulnérables (employé/employeurs) pour la finalité visée (accès sécurisé au lieu de travail).
    - À l'inverse, par exemple, la Direction générale de la sécurité intérieure (Ministère de l'Intérieur), serait fondée à permettre l'accès au bâtiment sur reconnaissance faciale de ses employés (données biométriques) au regard du niveau de sécurité attendu pour ce type bâtiment.

- Délai de conservation envisagé
  - Le RGPD impose aux responsables de traitement de fixer eux-mêmes la durée de conservation des données. C’est un élément majeur de protection. La durée pendant laquelle vous traitez des données personnelles doit forcément être limitée dans le temps. C’est à vous de fixer cette durée et de justifier ce délai (article 5 RGPD).
  - Par exemple, dans son avis du 10 novembre 2022, la CNIL a relevé que la société DISCORD INC. n’avait pas mis à disposition de ses utilisateurs une politique écrite indiquant la durée de conservation des données ou le critère pour calculer ce délai et que la société conservait, à tort, les données d’utilisateurs inactifs depuis plus de 3 ans.
  - Au cours de la procédure, la société s’est mise en conformité avec une politique écrite de conservation de données prévoyant la suppression des comptes après deux ans d’inactivité de l’utilisateur ce qui a été jugé conforme par la CNIL.

Évaluation du respect des droits des personnes concernées.

Cette sous-étape a pour objet de documenter la manière dont l'entreprise respecte ou envisage de respecter les droits que les personnes tirent du RGPD.

Voici les questions auxquelles vous devrez apporter des réponses précises :

- Comment les personnes sont-elles informées du traitement de leurs données personnelles ?
  - Vous retrouverez la liste des droits des personnes à l'article 13 RGPD qui prévoit notamment un droit à l'information. A titre d'illustration, pour reprendre l'exemple vu plus haut, les utilisateurs doivent avoir accès à la politique de conservation de leurs données.
- Comment le consentement est-il recueilli (si telle est la base légale retenue) ?
  - Pour rappel, le consentement doit pouvoir être exprimé de manière libre et expresse (article 7 RGPD et article 8 RGPD).

- Comment les personnes concernées peuvent exercer leurs droits ?
    - Le droit d’accès permet à un utilisateur de savoir où en est le traitement de ses données (article 15 RGPD).
    - Le droit de rectification permet la modification et la correction des données personnelles (article 16 RGPD).
    - Le droit d’opposition permet de s’opposer à l’utilisation de ses données pour un objectif précis (article 21 RGPD).
    - Le droit à l’effacement permet d’obtenir l’effacement de ses données (article 17 RGPD).
    - Le droit à la limitation permet d’arrêter temporairement l’utilisation des données (article 18 RGPD).
    - Le droit à la portabilité permet à la personne de récupérer une partie de ses données dans un format lisible pour son usage personnel ou pour les transmettre à un autre organisme d’assurance par exemple (copie des données) (article 20 RGPD).
- À quel sous-traitant ces données personnelles sont-elles transférées ? Quel est le contenu du contrat avec ce sous-traitant ? Que prévoit-il?

Étape n°3 - Évaluer les risques pour les droits et libertés des personnes.

Après l’analyse du traitement, il est nécessaire d’en tirer des conclusions sur l’évaluation du risque engendré par le traitement sur la vie privée des personnes.

Le responsable de traitement doit s’interroger sur la source du risque, la probabilité qu’il survienne et ses éventuelles conséquences pour les droits et libertés des personnes concernées par le traitement projeté.

Le risque peut être de nature diverse :

- Il peut provenir d’un niveau de sécurité trop faible de nature à engendrer une violation des données personnelles.
    - Par exemple : piratage informatique, faille des systèmes informatiques, surchauffe des serveurs, inondations des serveurs.
    - La source de la violation de la sécurité des systèmes peut être humaine : mot de passe trop faible, cambriolage des locaux professionnels et vols des dossiers papiers, vente des données par un collaborateur, vol de l’ordinateur d’un collaborateur.

- Il peut également provenir de l'objet du traitement.
    - Par exemple lorsque le traitement a pour objet des personnes vulnérables, données sensibles (informations relatives à l'origine raciale, politique, religieuse, données de santé etc.), perçues comme sensibles (données bancaires) ou relatives à des sanctions pénales.
- Le risque peut également provenir de la nature même du traitement.
    - Par exemple, lorsque l'organisme utilise un logiciel qui applique un algorithme pour analyse des données. Cette technologie peut conduire à opérer un profilage.

En tout état de cause, il convient d'identifier :

1. La source du risque. Par exemple la faille d'un système informatique.
2. L'aptitude du risque à survenir. Par exemple un risque élevé à la suite de constat de bug récurrent du système.
3. Les conséquences sur les droits et libertés des personnes si le risque vient à se réaliser. Par exemple si des données bancaires de clients sont conservées sur un cloud partagé à tous les employés, il existe un risque de divulgation de ces données bancaires à un tiers. Il existe un risque d'usurpation d'identité et de manipulation des données bancaires par des tiers non autorisés.

Pour vous aider à apprécier la gravité du risque, la CNIL a publié un tableau avec 4 niveaux de risque selon les situations.

Niveau 1 :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemples d'impacts moraux
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	* Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle) * Maux de tête passagers	* Perte de temps pour réitérer des démarches ou pour attendre de les réaliser * Réception de courriers non sollicités (ex. : spams) * Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) * Publicité ciblée pour des produits de consommation courants	* Simple contrariété par rapport à l'information reçue ou demandée * Peur de perdre le contrôle de ses données * Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale) * Perte de temps pour paramétrer ses données * Non-respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné)

Niveau 2 :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemples d'impacts moraux
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	* Affection physique mineure (ex. : maladie bénigne suite au non-respect de contre-indications) * Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) * Diffamation donnant lieu à des représailles physiques ou psychiques	* Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement * Refus d'accès à des services administratifs ou prestations commerciales * Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) * Promotion professionnelle manquée * Compte à des services en ligne bloqué (ex. : jeux, administration) * Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées * Élévation de coûts (ex. : augmentation du prix d'assurance) * Données non mises à jour (ex. : poste antérieurement occupé) * Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) * Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) * Profilage imprécis ou abusif	* Refus de continuer à utiliser les systèmes d'information (whistleblowing, réseaux sociaux) * Affection psychologique mineure mais objective (diffamation, réputation) * Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) * Sentiment d'atteinte à la vie privée sans préjudice irrémédiable * Intimidation sur les réseaux sociaux

Niveau 3 :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemples d'impacts moraux
3. Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	* Affection physique grave causant un préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non-respect de contre-indications) * Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.	* Détournements d'argent non indemnisé * Difficultés financières non temporaires (ex. : obligation de contracter un prêt) * Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen) * Interdiction bancaire * Dégradation de biens * Perte de logement * Perte d'emploi * Séparation ou divorce * Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage / phishing) * Bloqué à l'étranger * Perte de données clientèle	* Affection psychologique grave (ex. : dépression, développement d'une phobie) * Sentiment d'atteinte à la vie privée et de préjudice irrémédiable * Sentiment de vulnérabilité à la suite d'une assignation en justice * Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression) * Victime de chantage * Cyberbullying et harcèlement moral

Niveau 4 :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemples d'impacts moraux
4. Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	* Affection physique de longue durée ou permanente (ex. : suite au non respect d'une contreindication) * Décès (ex. : meurtre, suicide, accident mortel) * Altération définitive de l'intégrité physique	* Péril financier * Dettes importantes * Impossibilité de travailler * Impossibilité de se reloger * Perte de preuves dans le cadre d'un contentieux * Perte d'accès à une infrastructure vitale (eau, électricité)	* Affection psychologique de longue durée ou permanente * Sanction pénale * Enlèvement * Perte de lien familial * Impossibilité d'ester en justice * Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

Gravité, vraisemblance... Avec ces informations, vous êtes en mesure d'apprécier la nature acceptable (ou non) des risques liés à vos traitements et d'envisager les mesures adéquates (étape n°4).

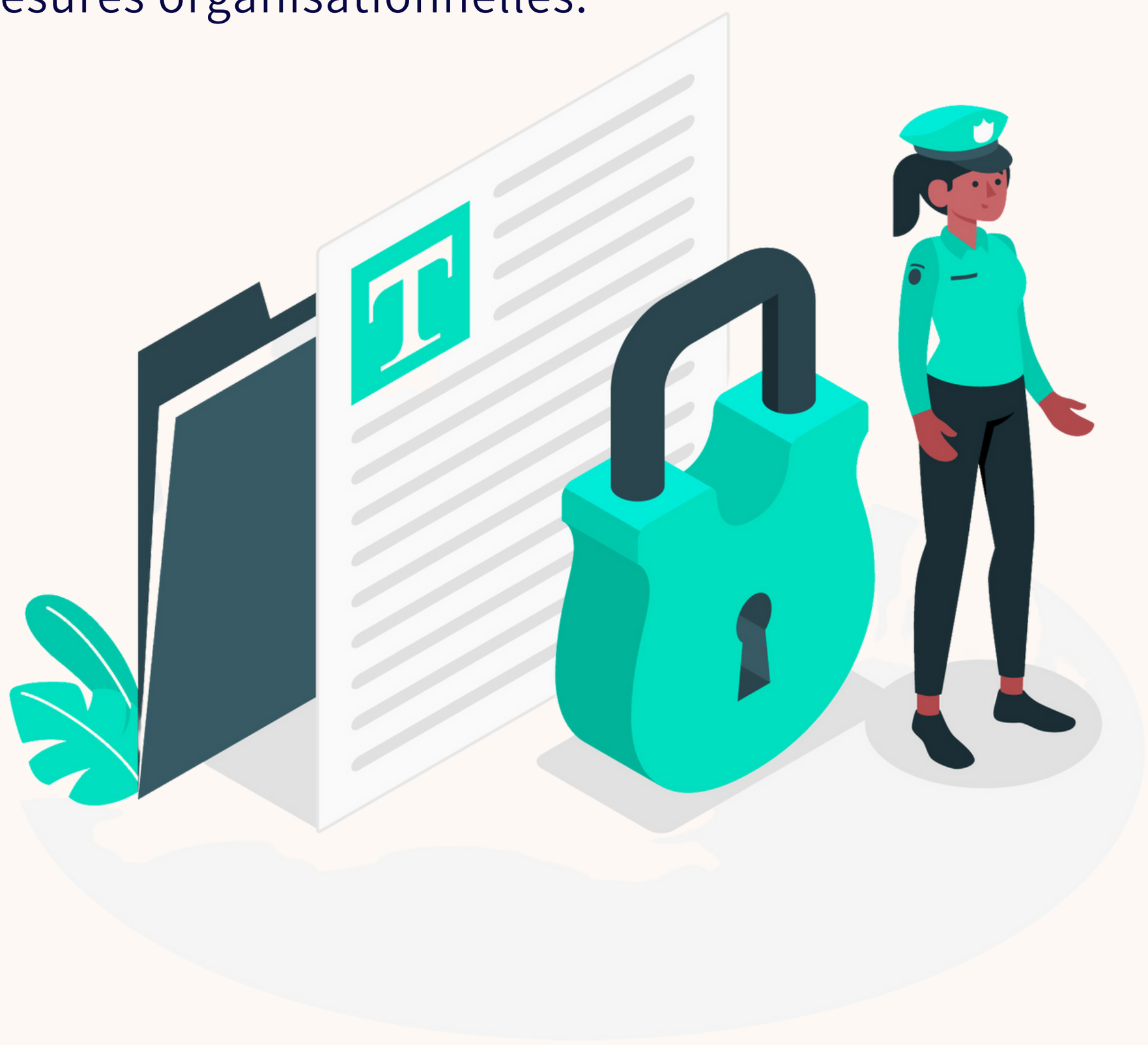
Étape n°4 - Mesures envisagées.

La dernière étape du PIA consiste logiquement à prévoir des mesures de sécurité pour réduire efficacement les risques identifiés. Ces mesures de sécurité doivent en particulier permettre (article 35 RGPD) :

- De réduire le risque pour le ramener à un niveau acceptable pour les personnes concernées,
- Et apporter la preuve du respect du RGPD.

Pour vous aider à choisir la mesure de sécurité la plus adaptée aux traitements envisagés, il peut être utile de se référer à l'article 32 RGPD qui établit une liste (non-exhaustive) de mesures qui peuvent être envisagées.

Il en existe deux types : les mesures techniques et les mesures organisationnelles.



Les mesures techniques :

- La pseudonymisation est l'action par laquelle un responsable de traitement relie des données personnelles non plus à l'identité de la personne concernée mais un pseudo ne permettant pas de l'identifier sauf à procéder à un recoupement d'informations supplémentaires (article 4 RGPD).
- L'anonymisation, à la différence de la pseudonymisation, ce processus anéanti définitivement toute possibilité de relier ces informations à la personne concernée par la donnée. En réalité, il ne s'agit plus de données personnelles, ces données sortent donc du champ même du RGPD.
- Le chiffrement des données est un dispositif empêchant la lecture des données par des tiers sauf à disposer de moyens techniques extrêmement techniques et coûteux.
    - Dans une affaire récente, Doctolib a été poursuivi concernant l'hébergement de ses données sur les serveurs de la filiale d'Amazon AWS (entreprise américaine, non conforme au RGPD). Néanmoins, le Conseil d'Etat a considéré que le risque était nettement réduit par la mise en place d'un dispositif de chiffrement des données par Doctolib. Attention, ce dispositif n'a de but que si la clé pour déchiffrer les données n'est pas dans les mains du sous-traitant à qui sont transférées les données chiffrées.

    - Pour plus d’information à ce sujet, nous avons rédigé un article ici.
- Les moyens techniques permettant d’assurer la disponibilité des données. Il s’agit de mesures protégeant les données de toute destruction ou altération en cas de dangers physiques tels que des incendies ou inondations.

Les mesures organisationnelles :

Ces mesures relèvent plus du facteur humain et visent à assurer que les personnes physiques qui travaillent sous l’autorité du responsable de traitement, ne traitent les données personnelles que sur leurs instructions.

Par exemple, une mesure organisationnelle consiste à soumettre les employés de l’entreprise ou du sous-traitant à une obligation de confidentialité (article 28 RGPD) ou encore de réserver l’accès à certaines données à un nombre limité de personnes dans l’entreprise.

Une autre mesure organisationnelle consiste à prévoir des ateliers de sensibilisation des collaborateurs à la protection des données personnelles. Mieux informés, vos employés auront les bons réflexes pour collecter le moins de données possibles, les conserver pendant une durée limitée ou encore être vigilant en matière de cybersécurité.

En plus des mesures techniques et organisationnelles, le responsable de traitement a tout intérêt à prévoir une procédure visant à tester régulièrement l'efficacité des mesures de sécurité. En effet, comme déjà évoqué, le PIA est un processus qui se construit sur la durée et évolue en fonction de l'activité de l'entreprise et des technologies utilisées.

Enfin, documentez tous ces éléments de la manière la plus précise possible.

Pour plus de détails sur l'ensemble des mesures techniques et organisationnelles envisageables dans un PIA, la CNIL a détaillé ces mesures dans un livrable.

Faut-il consulter la CNIL au préalable ?

L’article 36 RGPD prévoit que le responsable de traitement consulte la CNIL préalablement au traitement lorsque la conclusion d’une analyse d'impact révèle que le traitement présenterait un risque élevé si le responsable du traitement ne prenait **pas de mesures pour atténuer le risque.**

C'est-à-dire que la CNIL doit être consultée lorsque les risques identifiés ne peuvent pas être réduits à un niveau acceptable par le responsable du traitement ou qu’il n’arrive pas à prévoir de mesures suffisantes. Il s’agit d’un risque résiduel lorsqu’il a des conséquences graves pour les droits et libertés des personnes. Dans ce cas, la consultation est obligatoire.

Un exemple de risque résiduel grave, selon le G29, consisterait en un accès non autorisé aux données personnelles qui pourraient entraîner une mise à pied, une mise en péril de leur situation financière ou qu’il existe une très forte probabilité que le risque se réalise.

Quoi qu’il en soit, votre décision doit être formalisée et documentée (graphiques des risques, plan d'actions des mesures mises en œuvre, délais de réalisation...).

Faut-il publier son PIA ?

Rien n’interdit le responsable de traitement de publier son PIA et rien de l’y oblige. La décision de publier son PIA relève de la liberté du responsable de traitement.

Néanmoins, pour votre activité, il peut être très intéressant de publier la conclusion de votre PIA pour générer la confiance de vos utilisateurs, clients et employés.

Une déclaration sur le résultat de votre PIA et votre volonté de protéger au mieux les données personnelles est également un argument business très important. Il ne faut pas l’oublier, votre conformité au RGPD est un atout concurrentiel majeur !

5. CONCLUSION

Le PIA est votre meilleur atout business.

CONCLUSION

Certes, la réalisation d’une analyse d’impact est un processus qui demande du temps et de la rigueur. C’est un enjeu de taille. Néanmoins, le jeu en vaut la chandelle !

Ce document démontre votre capacité à réaliser des opérations de traitements éthiques et responsables. Il vous aide à vous projeter dans l’avenir et à développer une aptitude à protéger la vie privée des personnes qui vous confient leurs données.

Votre réputation est en jeu. Une fuite d'informations sensibles liée à l’absence de PIA ou PIA bâclée risquerait de mettre en péril la poursuite de votre activité.

Aussi, n’hésitez pas à publier votre PIA (même si cela n'est pas obligatoire). Vous prouvez à nouveau votre sérieux et votre souci de transparence. Les personnes concernées apprécieront votre démarche, se sentiront en confiance.

Un vrai plus pour un business pérenne.

Des interrogations ? N’hésitez pas à nous contacter !

LETO.LEGAL

CONTACTEZ-NOUS

VOUS ÊTES À DEUX DOIGTS DE VOTRE CONFORMITÉ

E-MAIL :
contact@leto.legal

SITE WEB :
leto.legal