

Fiche savoir 0 MOOC RGPD de la CNIL

(version hors ligne et synthétique)



1	Module 1 RGPD et notions clés.....	2
1.1	Principes	2
1.2	A qui s'applique le RGPD	7
2	Module 2 Les principes de protection des données personnelles.....	9
2.1	Données sensibles	9
2.2	Sécurisation	10
2.3	Droits sur les données	12
3	Module 3 La responsabilité des acteurs	13
3.1	Synthèse	13
3.2	Sous-traitance.....	15
4	Module 4 Le DPO et les outils de la conformité	16
4.1	DPO	16
4.2	Le registre	18
4.3	L'analyse d'impact	20
4.4	Notification de violation des données	26

1 Module 1 RGPD et notions clés

1.1 Principes

Afin de garantir à la vie privée et aux libertés des personnes un niveau de protection maximal, **le RGPD s'articule autour de trois axes majeurs** :

1

Le renforcement quantitatif et qualitatif des droits des personnes.

2

Une nouvelle logique de responsabilisation de l'ensemble des acteurs des traitements de données.

3

Le renforcement des pouvoirs de sanction des CNIL européennes.

INTRODUCTION

Le RGPD encadre la mise en œuvre des traitements de données à caractère personnel. Il fixe les conditions dans lesquelles de telles données peuvent être légalement collectées, conservées et exploitées par les organismes.

Ces conditions visent à éviter que l'utilisation des informations en cause porte atteinte aux droits et libertés des personnes qu'elles concernent.

LES DONNÉES À CARACTÈRE PERSONNEL

RGPD - Article 4

“

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.

”



1 Des données **directement** identifiantes

Les données personnelles sont directement identifiantes **si elles sont associées à un élément indiquant clairement l'identité de la personne**. Il peut s'agir d'un nom, d'un prénom, d'un email nominatif, d'une photo, etc.

Ce type de données figure, par exemple, sur :

- les fiches de paie
- les relevés de compte bancaire
- les devis
- les factures
- les fichiers clients
- etc.

2 Des données **indirectement** identifiantes

Dans certains fichiers, les noms et prénoms des personnes sont remplacés par un identifiant : numéro client, numéro de téléphone, etc.

Prises isolément, ces données ne permettent pas de savoir immédiatement à qui correspondent les informations.

En revanche, **lorsqu'elles sont associées à une autre base de données** détenue en interne ou par tout autre tiers, comme le fichier client de l'entreprise ou l'annuaire téléphonique, **il est possible de retrouver l'identité de la personne**.

LES DONNÉES À CARACTÈRE PERSONNEL

3 Les combinaisons d'informations

Certaines informations ne permettent pas à elles seules ni directement, ni indirectement (en étant associées à une autre base) d'identifier une personne.

En revanche, **la combinaison de plusieurs de ces informations peut parfois permettre d'identifier de manière unique une seule personne.**

LES DONNÉES À CARACTÈRE PERSONNEL

Parmi ces données, laquelle ou lesquelles ne sont pas des données personnelles ?

Un numéro de plaque
d'immatriculation

Des coordonnées
d'entreprise

Un numéro
de carte de paiement

Des images
de vidéosurveillance

Parmi ces propositions, seules les coordonnées d'une entreprise ne sont pas considérées comme des données personnelles. Il s'agit de données génériques (adresse postale, numéro de téléphone du standard, email de contact générique, etc.) qui ne correspondent pas à un individu. Attention : certaines données non nominatives peuvent toutefois être identifiantes. Par exemple, le Directeur des ressources humaines de la société X.

TRAITEMENT

RGPD - Article 4

“

Est un traitement **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 [...]

”

TRAITEMENT

Sont ainsi notamment concernées les opérations suivantes :

- la collecte
- l'enregistrement
- la structuration
- la conservation (l'hébergement)
- la transmission
- la modification
- l'extraction
- la communication
- la mise à disposition
- le rapprochement
- etc.

Le traitement de données personnelles est très vite arrivé !

Fermer les exemples



Entrer les coordonnées d'un nouveau prospect dans le logiciel de gestion commerciale.



Extraire une liste des clients n'ayant pas passé commande depuis plus de 3 mois.

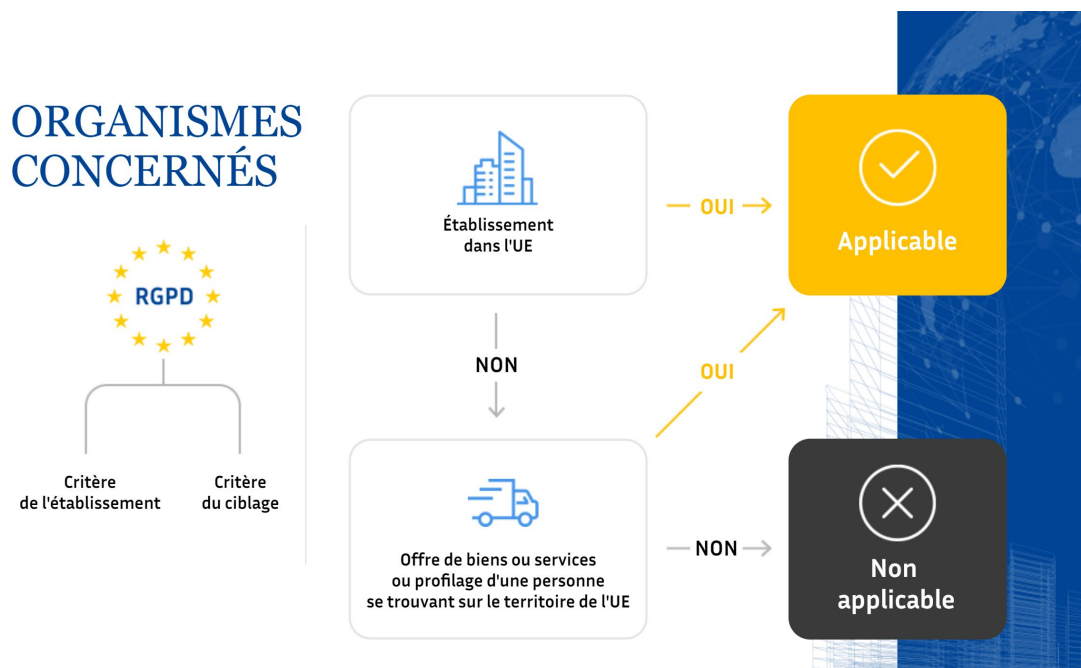


Utiliser les numéros de téléphone des clients en question pour les appeler et les informer d'une nouvelle offre promotionnelle.



Faire un devis à chaque client intéressé suite à l'appel.

1.2 A qui s'applique le RGPD



RESPONSABLE DE TRAITEMENT ET SOUS-TRAITANT

Tous deux concernés par le RGPD.

- plus généralement, tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme.

SYNTHÈSE

Tout organisme est concerné par le RGPD dès lors qu'il se trouve sur le territoire de l'UE ou qu'il traite des données personnelles d'individus se trouvant sur le territoire de l'UE.

2 Module 2 Les principes de protection des données personnelles

4 bons réflexes (8 règles d'or) :

- données strictement nécessaires = finalité ?
- transparence
- accès, rectification, suppression des données
- sécurisation des données

2.1 Données sensibles

INTRODUCTION

Il s'agit de données **particulièrement sensibles** **du point de vue des libertés et des droits fondamentaux.**

Ce sont des données qui touchent à l'intimité de l'individu, voire à l'identité humaine, et dont l'utilisation pour un mauvais usage représente un risque élevé pour les personnes.

Le traitement de ces données ne peut donc se faire sans le respect d'un cadre juridique strict.

Ces données à risque sont :

- les données dites « sensibles »
- le numéro de sécurité sociale (NIR)
- les données personnelles relatives aux condamnations pénales, aux infractions et aux mesures de sûreté.

Tout traitement, comme la collecte ou la consultation, de données dites « sensibles » **est par principe interdit** par le RGPD puisque ces données sont relatives à l'intimité de la vie privée.

Les données sensibles sont celles qui révèlent ou concernent :

- | | |
|---|---|
| ■ les origines raciales ou ethniques | ■ la santé (physique ou mentale) |
| ■ les opinions politiques | ■ la vie sexuelle ou l'orientation sexuelle |
| ■ les convictions philosophiques ou religieuses | ■ les données génétiques |
| ■ l'appartenance syndicale | ■ les données biométriques aux fins d'identifier une personne physique de manière unique. |

Les 8 r gles d'or

- Lic t  du traitement
- Finalit  du traitement
- Minimisation des donn es
- Protection particuli re des donn es sensibles
- Conservation limit e des donn es
- Obligation de s curit 
- Transparence
- Droits des personnes

DÉFINITION

RGPD - Article 32-1

“

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, **le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins :

- A** la pseudonymisation et le chiffrement des données à caractère personnel
- B** des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement
- C** 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
- D** 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 3 principes de la sécurité

Pour être pleinement prise en compte, l'obligation de sécurité doit être appréhendée de manière globale, sous l'angle des 3 principes suivants :

- le principe de **confidentialité** : les données ne doivent être accessibles qu'aux personnes autorisées
- le principe d'**intégrité** : les données ne doivent pas être altérées ou modifiées
- le principe de **disponibilité** : les données doivent être en permanence accessibles par les personnes autorisées.

SYNTHÈSE

Assurer la protection des données à caractère personnel que l'on traite est essentiel.

L'obligation de sécuriser les données doit conduire les acteurs concernés (responsables de traitements et sous-traitants) à mettre en place les mesures physiques, logiques et organisationnelles qui s'imposent.

Ces mesures devront être adaptées au contexte et, le cas échéant, réajustées en fonction de l'évolution des risques.

2.3 Droits sur les données

INTRODUCTION

L'un des objectifs majeurs du RGPD est de renforcer les droits des personnes et de faciliter leur exercice.

Aux droits d'accès, de rectification, d'effacement et d'opposition qui se voient renforcés viennent s'ajouter de nouveaux droits.

Ces nouveaux droits sont le droit à la portabilité, le droit à la limitation du traitement et le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé.

3 Module 3 La responsabilité des acteurs

3.1 Synthèse

SYNTHÈSE

La responsabilisation des acteurs est au cœur de la conformité au RGPD.

Afin d'assurer une protection optimale des données personnelles qu'ils traitent, les acteurs (responsables de traitements et sous-traitants) doivent mettre en place, de manière continue, des mesures de protection des données appropriées et démontrer cette conformité à tout moment (« *accountability* »).

Responsabilité =>

- appliquer des mesures de protection
 - dès la conception
 - par défaut
 - = limiter au strict nécessaire dès la conception
- documenter les mesures

⇒ les outils

Il existe deux catégories d'outils

1

Les outils **obligatoires**

- le registre des activités de traitement
- le délégué à la protection des données dans certains cas
- l'analyse d'impact pour certains traitements
- la notification de violations de données sous certaines conditions.

2

Les outils **recommandés**

- la certification
- les codes de conduite
- les règles d'entreprise contraignantes (BCR)
- etc.

LES OBLIGATIONS

Le sous-traitant est soumis à quatre types d'obligation.

- 1 Transparence
et traçabilité
- 2 Sécurité
des données traitées
- 3 Encadrement de la
sous-traitance ultérieure
- 4 Accompagnement
du responsable de traitement

4 Module 4 Le DPO et les outils de la conformité

4.1 DPO

MISSIONS

1 Informer
et **conseiller** l'organisme

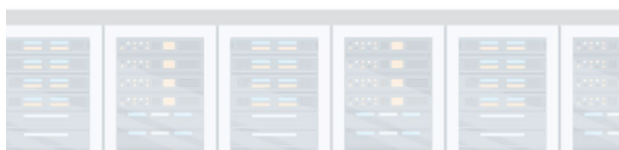
2 Contrôler
la conformité

3 Jouer un rôle d'interface
entre l'organisme, la CNIL
et les personnes concernées

MISSIONS

2 Contrôler
la conformité

Pour chacune des activités de traitement, sur la base des éléments figurant dans le registre et des audits qu'il pourra mener pour les vérifier ou les compléter, **le délégué devra s'assurer du respect des différents principes de protection des données :**



- elles disposent bien d'une base juridique (obligation légale, contrat, intérêt légitime, mission d'intérêt public, consentement des personnes, etc.)
- seules les données strictement nécessaires à la satisfaction de l'objectif poursuivi sont collectées
- les personnes concernées disposent d'un niveau d'information suffisant
- leurs réclamations sont effectivement prises en compte
- les opérations sous-traitées à des prestataires sont dûment encadrées
- les données sont exploitées dans des conditions garantissant leur intégrité, leur disponibilité et leur confidentialité
- celles qui ne sont plus d'utilisation courante par les services opérationnels sont bien détruites, anonymisées ou archivées.

Désignation obligatoire

Il existe **trois cas** pour lesquels la désignation d'un délégué est obligatoire :

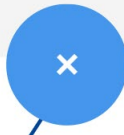
1er cas : les autorités et organismes publics.

Par nature, toutes les autorités nationales, régionales et locales doivent se doter d'un délégué. Il s'agit en particulier des services de l'État, des collectivités territoriales et de leurs groupements, ainsi que de leurs établissements publics.



2e cas : les organismes privés dont...

les **activités de base** les amènent à réaliser un **suivi régulier et systématique** des personnes à **grande échelle**.



3e cas : les organismes privés dont...

les **activités de base** les amènent à traiter à **grande échelle** des **données dites « sensibles »** ou relatives à des condamnations pénales et infractions.



4.2 Le registre

INTRODUCTION

Un registre des activités de traitement doit être mis en place par tout responsable de traitement ou sous-traitant.

Outil essentiel dans les opérations de conformité, il permet de recenser les traitements, et par la même occasion, de disposer d'une vue d'ensemble sur ce qui est fait des données personnelles dans les organisations.

Organismes concernés

L'obligation de tenir un registre des traitements concerne tous les organismes, publics comme privés, quelle que soit leur taille, dès lors qu'ils traitent des données personnelles.

Le registre doit être tenu par les responsables de traitement et les sous-traitants eux-mêmes.

Cette mission peut être confiée au délégué à la protection des données, même s'il est externalisé, ou à une autre personne en interne.



Contenu

Le registre est un **document de recensement et d'analyse**, il doit refléter la réalité des traitements et permettre d'identifier précisément :

- les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données
- les catégories de données traitées
- à quoi servent les données
- qui accède aux données et à qui elles sont communiquées
- combien de temps elles sont conservées
- comment elles sont sécurisées

La liste détaillée des éléments à intégrer au registre du responsable de traitement et du sous-traitant est disponible sur le site de la CNIL.

Dérogation

Les entreprises de moins de 250 salariés bénéficient d'une dérogation. Elles sont autorisées à n'inscrire dans le registre que les traitements suivants :

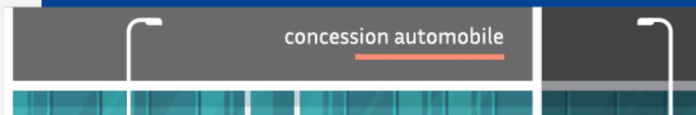
- **les traitements récurrents**
(ex: gestion de la paie, gestion des clients, des prospects et des fournisseurs, etc.)
- **les traitements susceptibles de comporter un risque pour les droits et libertés des personnes**
(ex: systèmes de géolocalisation, de vidéosurveillance, etc.)
- **les traitements qui portent sur des données sensibles**
(ex: données de santé, infractions, etc.).

Exemple :

Un concessionnaire automobile décide de lancer une campagne de communication à l'occasion de l'ouverture d'un nouvel établissement.

Les traitements liés à cette campagne n'ont pas besoin d'être intégrés au registre puisqu'il s'agit d'un événement ponctuel dont le traitement ne représente aucun risque pour les personnes concernées.

En cas de doute sur l'application de cette dérogation, la CNIL recommande d'intégrer le traitement au registre.



⇒ voir modèle de registre

Méthode :

- 1- rassembler infos dispo
- 2- élaborer la liste des traitements
- 3- affiner

4.3 L'analyse d'impact

L'AIPD est un outil central permettant la mise en œuvre concrète du principe de responsabilisation des organismes :

- elle aide à construire des traitements de données respectueux de la vie privée
- elle permet de démontrer sa conformité au RGPD.

Objectifs

- décrire les traitements
- évaluer conformité rgpd
- identifier les risques
- réduire les risques

Définition de risque pour la vie privée :

C'est un scénario qui décrit :

- **un événement redouté**, comme l'accès illégitime à des données, la modification des données ou leur disparition
- **toutes les menaces qui rendent cet événement possible** (ex : vol d'un ordinateur portable, contagion d'un logiciel par un code malveillant, manipulation inopportune lors de configuration d'un logiciel, etc.)
- **la source de cette menace** (ex: un salarié, un hacker, un virus, etc.)
- **les impacts potentiels de cet événement** sur les personnes concernées (ex : perte d'emploi, piratage d'un compte bancaire, etc.)

Le risque est estimé par une appréciation :

- de sa **gravité** : quelle est l'ampleur du préjudice pour les personnes concernées ?
- et de sa **vraisemblance** : quelle est la chance que l'évènement redouté se réalise ?

Quels sont les traitements concernés par l'AIPD ?

La réalisation d'une AIPD est obligatoire lorsque le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques » (article 35 du RGPD).

En cas de doute quant à la nécessité d'effectuer une AIPD, il est conseillé d'en effectuer une dans la mesure où elle représente une méthodologie complète de mise en conformité du traitement.

Elle est facultative dans tous les autres cas.

AIPD obligatoire

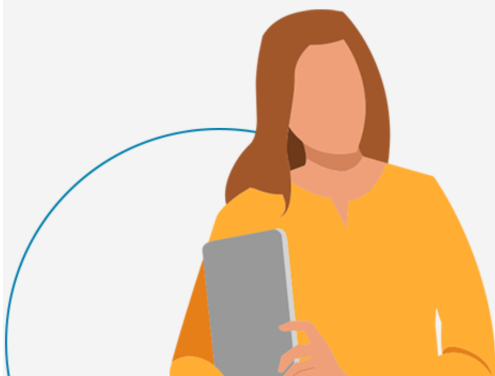
C'est au responsable de traitement de déterminer si un ou plusieurs des traitements qu'il met en œuvre présentent un **risque élevé pour les droits et libertés des personnes**.

Pour cela, il convient de vérifier si :

- 1** Il correspond à l'un des trois traitements visés à l'article 35-3 du RGPD
- 2** Il figure sur la liste élaborée par la CNIL des traitements pour lesquels une AIPD est requise
- 3** Il remplit un ou plusieurs des critères listés par le Comité européen de la protection des données (CEPD) dans ses lignes directrices concernant l'analyse d'impact

AIPD OBLIGATOIRE

1 Les **trois traitements** visés à l'article 35-3 du RGPD



■ l'évaluation systématique et approfondie d'aspects personnels

concernant des personnes physiques, fondée sur un traitement automatisé (y compris le profilage), 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.

Ex: un traitement entièrement automatisé évaluant le profil d'un candidat à un recrutement et pouvant aboutir à un refus sans aucune intervention humaine.

■ le traitement à grande échelle de catégories particulières de données sensibles, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Ex: un traitement des données de santé par un hôpital dans le cadre de la prise en charge des patients.

■ la surveillance systématique à grande échelle

d'une zone accessible au public.

Ex: un dispositif de vidéosurveillance mis en place par un opérateur ferroviaire dans l'ensemble de ses gares.

AIPD OBLIGATOIRE

2 La liste des traitements pour lesquels une AIPD est requise

La CNIL a publié une liste des opérations de traitements pour lesquels elle estime obligatoire qu'une AIPD soit réalisée ([document accessible sur le site de la CNIL](#)).



Elle comporte 14 types d'opérations de traitement parmi lesquels figurent, par exemple :

- Les traitements établissant des **profils de personnes physiques** à des fins de gestion des ressources humaines (ex : traitement de détection et de gestion de « hauts potentiels », traitement visant à faciliter le recrutement, notamment grâce à un algorithme de sélection, etc.)
- Les traitements impliquant le **profilage des personnes** pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci (ex: traitement établissant un score pour l'octroi de crédit, traitement de lutte contre la fraude aux moyens de paiement, etc.)

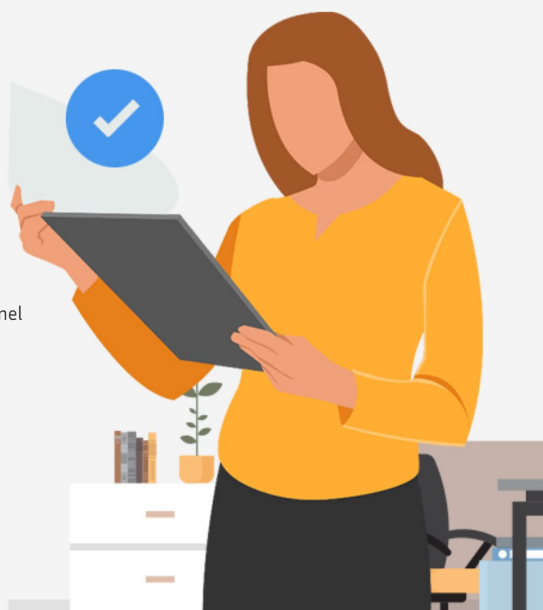
AIPD OBLIGATOIRE

3 Les critères des lignes directrices

Les critères issus des lignes directrices du CEPD sont les suivants :

- évaluation (y compris le profilage)
- décision automatique avec effet légal ou similaire
- surveillance systématique
- collecte de données sensibles ou données à caractère hautement personnel
- collecte de données personnelles à grande échelle
- croisement de données
- personnes vulnérables (patients, personnes âgées, enfants, etc.)
- usage innovant (utilisation d'une nouvelle technologie)
- exclusion du bénéfice d'un droit ou d'un contrat

Dans la plupart des cas, le responsable du traitement peut considérer qu'un traitement qui satisfait à deux critères nécessite une AIPD.



Exemples

1

2

Une entreprise met en place un traitement publicitaire visant à collecter les données de géolocalisation de plusieurs millions d'individus pour créer des profils publicitaires et leur afficher de la publicité ciblée en fonction de leurs déplacements.

Ce traitement remplit les critères de la collecte à grande échelle, celui de la collecte de données à caractère hautement personnel (les données de localisation) et celui de la surveillance systématique.

Une analyse d'impact doit donc dans ce cas être réalisée.

Exemples

1

2

Un établissement médico-social (ex. CCAS, EHPAD) met en place un traitement de prise en charge de la santé de personnes vulnérables. Ce traitement remplit les critères de la collecte de données sensibles (données de santé), et celui relatif à la vulnérabilité des personnes concernées.

Le responsable de traitement devra mener une analyse d'impact pour ce traitement.

Contenu

L'analyse d'impact doit contenir *a minima* :

- une **description systématique** des opérations de traitement envisagées et les finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement
- une **évaluation de la nécessité et de la proportionnalité** des opérations de traitement au regard des finalités
- une **évaluation des risques sur les droits et libertés** des personnes concernées
- les **mesures envisagées** pour faire face aux risques, y compris les mesures et mécanismes de sécurité visant à assurer la protection des données personnelles et à apporter la preuve du respect du règlement.

Méthode

L'analyse d'impact doit être réalisée avant la mise en œuvre du traitement.

Elle doit être amorcée le plus en amont possible et mise à jour tout au long du cycle de vie du traitement.

Pour ce faire, le responsable de traitement peut choisir librement une méthode, à condition qu'elle respecte les critères des lignes directrices dédiées à la réalisation d'une AIPD.

La CNIL a développé un logiciel gratuit qui facilite la conduite et la formalisation d'une AIPD.

Découvrir le logiciel PIA



4.4 Notification de violation des données

Objet : confidentialité, disponibilité, intégrité

Définition

Pour qu'il y ait violation de données personnelles, deux conditions doivent être réunies :

- l'organisme a effectué un traitement de données personnelles
- ces données ont fait l'objet d'une **perte de disponibilité**, d'**intégrité** ou de **confidentialité**, de manière accidentelle ou illicite.



Délais de notification

À la CNIL

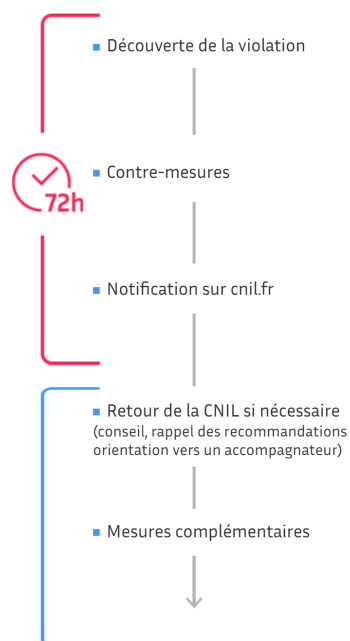
Si l'incident constitue un risque au regard de la vie privée des personnes concernées, l'organisme doit **notifier l'incident à la CNIL** via un formulaire disponible sur son [site internet](#).

Elle doit être effectuée dans les meilleurs délais, et si possible dans les 72 heures après la constatation de la violation des données personnelles.

L'organisme dispose d'un délai de 72h pour notifier à la CNIL

Elle doit également informer les personnes concernées dans les meilleurs délais selon les exigences du RGPD

Passé 72h, l'organisme s'expose à une mesure répressive



SYNTHÈSE

Pour les personnes concernées, la violation engendre :	aucun risque	un risque	un risque élevé
Documentation en interne par le RT sous forme d'un registre interne des différentes violations dont il est victime	×	×	×
Notification à l'autorité de contrôle, c'est-à-dire la CNIL en France, si possible en 72h		×	×
Information des personnes concernées dans les meilleurs délais, hors cas particuliers			×