RGPD

Passez à l'action

Amphithéâtre de la CCISM

Vendredi 7 mars 2019

De 14h à 18h30

esci

CCISM
POLYNÉSIE FRANÇAISE

DGEN
DIRECTION GENERALE DE L'ECONOMIE NUMERIQUE

OPEN
Organisation des Professionnels de l'Économie Numérique

CLUSIR
TAHITI

TAHITI NUI FORTRESS

DT
DIGITAL TAHITI

SPILOG
Partner Consulting Services

ACTECIL
RGPD SOLUTIONS

IAORA systems
SERVICES ET INGÉNIERIE INFORMATIQUES

Avec le RGPD, la sécurisation de vos données fait maintenant partie des principes à respecter (art. 6 à 11)

Principe 1	• Licéité, loyauté, transparence
Principe 2	• Limitation des finalités
Principe 3	• Minimisation des données
Principe 4	• Exactitude
Principe 5	• Limitation de conservation
Principe 6	• Garantir la sécurité des données

Nouveau

La disponibilité, l'intégrité et la confidentialité des données à caractère personnel doivent être garanties (même pour les données non sensibles)

Traitement à risque - les 9 critères à surveiller

l'**évaluation** ou notation d'une personne	une prise de **décision automatisée**	la **surveillance systématique** de personnes
le traitement de **données sensibles**	le traitement de données de **personnes vulnérables**	le traitement à **grande échelle** de données personnelles
le **croisement** d'ensembles de données	Usages **innovants** ou l'application de nouvelles technologies	l'**exclusion du bénéfice** d'un droit, d'un service ou contrat (ex : liste noire)

Un traitement est considéré à risque si il répond à **2 critères parmi les 9 listés**

Quelques exemples de traitements à risque fournis par la CNIL

La CNIL a publié sur son site une liste avec de traitements type à risque [1]

Données sensibles + personnes dites vulnérables

- traitements «de santé» mis en œuvre par les établissements de santé
- dossier « patients »
- algorithmes de prise de décision médicale ;
- dispositifs de vigilances sanitaires…

évaluation ou notation + croisement d'ensembles de données

- traitement établissant un score pour l'octroi de crédit
- traitement de lutte contre la fraude aux moyens de paiement …

A grande échelle + usage innovant

- Application mobile permettant de collecter les données de géolocalisation des utilisateurs
- mise en œuvre d'un système de billettique par des opérateurs de transport…

Utiliser l'analyse d'impact pour gérer vos risques

Mon traitement est **sur la liste CNIL** des cas pour lesquels une AIPD est obligatoire

Ou

Mon traitement remplit-il **2 critères parmi les 9** énoncés précédemment

Vous devez conduire une analyse d'impact sur la protection des données (AIPD) **avant de collecter** des données et sur les **traitements antérieurs au RGPD (l'existant)**

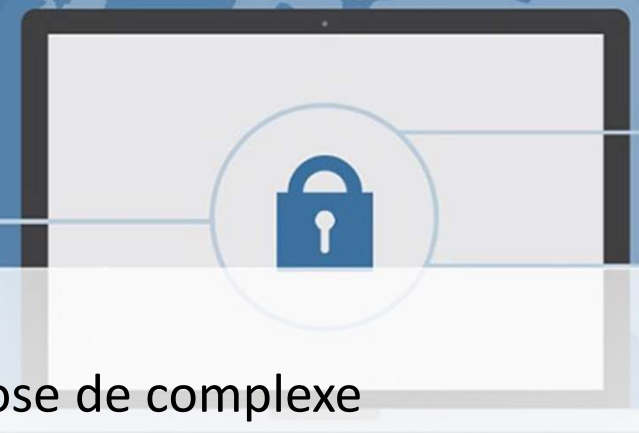
L'AIPD est une action pivot dans la démarche de conformité

Figure 1 – La démarche de conformité à l'aide d'un PIA

La CNIL propose des **guides méthodologiques et un outil gratuit**

https://www.cnil.fr/fr/PIA-privacy-impact-assessment
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

AIPD, quelle démarche ?



- Pragmatique!
  - Ne pas faire de l'AIPD quelque chose de complexe
  - Revoir votre gestion de projet pour intégrer l'AIPD avec vos méthodes existantes
  - Former les chefs de projet métiers, AMOA et informatique à votre approche sécurité
- Diversifiée !
  - Il n'y a pas un expert RGPD
  - Mixité des compétences : juridique, technique, sécurité, exploitation …
- Maitrisée !
  - Une chefferie de projet
  - Une priorisation des chantiers selon leur complexité (cout / mise en œuvre)

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance

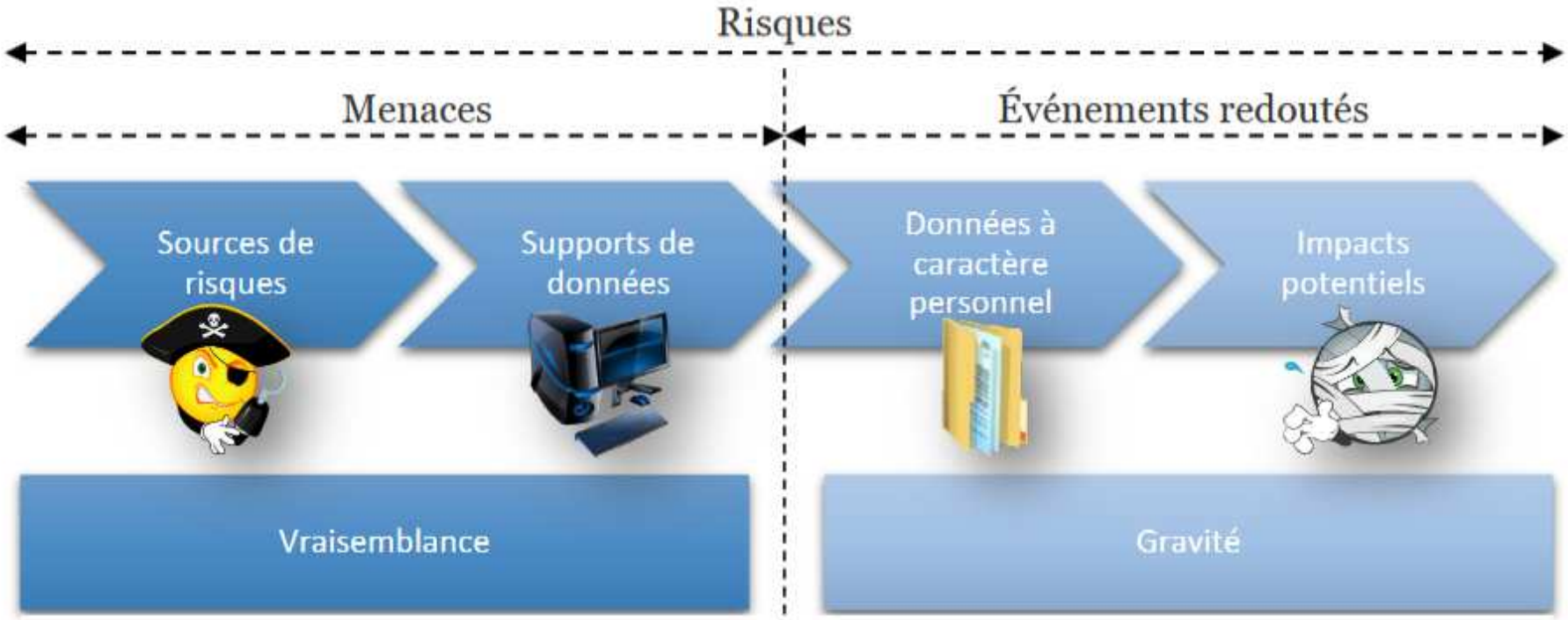


Figure 3 – Éléments composant les risques

Il faut alors sélectionner des mesures de sécurité **pour réduire ces risques**

Source : CNIL, CNIL-PIA-1-Méthode.pdf

Piocher dans la boite à outil des mesures de sécurité pour limiter vos risques

- S'appuyer sur les guides de la CNIL ou des **référentiels reconnus** et **combiner plusieurs thématiques** pour une meilleure défense en profondeur

Prévenir

- Sensibilisation
- Gérer les habilitations

Protéger

- Authentifier les utilisateurs
- Sécuriser les postes de travail
- Protéger les locaux

Contenir

- Séparer les réseaux d'administration
- Cloisonnement des données

Détecter

- Tracer les accès

Remédier

- Sauvegarder vos données
- Procédure de gestion d'incident

ANSSI

En cas d'incident, comment notifier la CNIL ?

- Obligation de notifier les incidents de sécurité auprès de la CNIL **sous 72h (art. 33)** en précisant:
  - La nature de la violation, et si faisable, le nombre de personnes concernées ;
  - Le nom du délégué à la protection des données (DPO) ;
  - Les problèmes que peuvent entrainer la violation des données ;
  - Les mesures prises ou que vous envisagez de prendre pour **remédier** à la violation, le cas échéant, des **mesures d'atténuation**.

- Pour de l'assistance https://www.cybermalveillance.gouv.fr/
- Pour notifier https://notifications.cnil.fr/notifications/index

Exception à la règle : la notification n'est pas obligatoire si les données sont impossibles à lire (données fortement chiffrées).

Faut-il notifier les personnes concernées ?

- L'obligation, dans certain cas, de communiquer auprès des personnes concernées (art. 34) de manière individuelle ou **publique**

En cas de doute, notifiez à la CNIL qui vous indiquera s'il est nécessaire d'informer les personnes.

- **Se préparer au pire pour être efficace en cas de crise**
  - Formaliser et tester les procédures internes de gestion des incidents (arbre de décision, message type …)
  - Inscrire le processus de gestion des incidents dans celui de la gestion de crise

MERCI

www.clusir-tahiti.org