DPIA : DPO, CHOISISSEZ LA PILULE ROUGE

ALESSANDRO FIORENTINO

Infhotep

Head of Personal Data Protection Practice

Product Owner de la plateforme Adequacy

Responsable de la formation DPO certifié Afnor

ISEP & Institut Mines Télécom

Data Protection Management Senior Lecturer – Institut Mines - Télécom

Personal Data Protection Lecturer – DPO Practices - ISEP

Member of Scientific Board of Data Protection Management Master - ISEP

QU’EST CE QU’UNE ANALYSE D’IMPACT RELATIVE À LA PROTECTION DES DONNÉES ?

QUOI ?	Des études de risques qui doivent être réalisées sur l'ensemble des traitements considérés comme sensibles (article 35).
POURQUOI ?	Les données personnelles traitées par les organismes sont vulnérables à divers risques : Accès Illégitime, Modification non désirée, Disparition
OBJECTIF	Aider à construire des traitements de données respectueux de la vie privée et démontrer leur conformité au RGPD.

CE QUI ÉTAIT PRÉVU

Une AIPD devait être réalisée	Une AIPD n'était pas exigée
Pour les traitements, antérieurs au 25 mai 2018 qui avaient fait l'objet d'une modification substantielle depuis l'accomplissement de leur formalité préalable	Pour les traitements qui avaient fait l'objet d'une formalité préalable auprès de la CNIL avant le 25 mai 2018, ou qui étaient dispensés de formalité
Pour tout nouveau traitement après le 25 mai 2018	Pour les traitements qui ont été consignés au registre d'un Correspondant « Informatique et libertés » (CIL)

Cette dispense d'obligation de réaliser une AIPD, pour les traitements existants et régulièrement mis en œuvre a été limitée à une période de 3 ans à compter du 25 mai 2018

QUESTION N°1

DOIS-JE FAIRE UNE AIPD ?

LA DÉMARCHE À SUIVRE

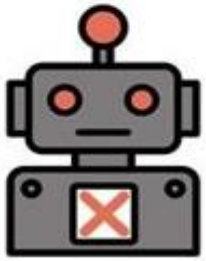
1) Mon traitement est-il présent dans l'une des deux listes publiées par la CNIL ?

- Liste des opérations de traitement pour lesquelles une AIPD était requise
- Liste des opérations de traitement pour lesquelles une AIPD n'était pas requise

2) Mon traitement remplit-il au moins deux des neuf critères issus des lignes directrices du Comité Européen de Protection des Données ?

Les 9 critères du G29

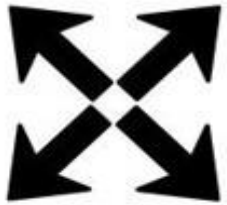
Evaluation ou Scoring



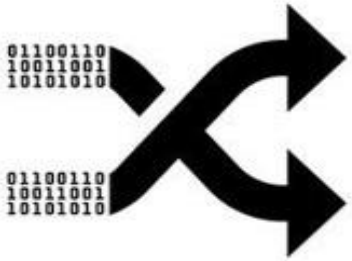
Décision automatique avec effet légal

Surveillance systématique

Données sensibles ou hautement personnelles



Large échelle



Croisement de données

Personnes vulnérables

Usage innovant

Exclusion d'un droit ou contrat

COMMENT RÉALISER UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES ?

L’ART. 35 INDIQUE CE QUE TOUT ANALYSE DOIT CONTENIR

Description

Une description systématique des opérations de traitement envisagées et des finalités de traitement

Nécessité

Une évaluation de la nécessité et de la proportionnalité des opérations au regard des finalités

Risques

Une évaluation des risques pour les droits et libertés des personnes concernées

Mesures

Les mesures envisagées pour faire face aux risques

Avis

L’avis du DPO et des personnes concernées ou de leurs représentants au sujet du traitement prévu

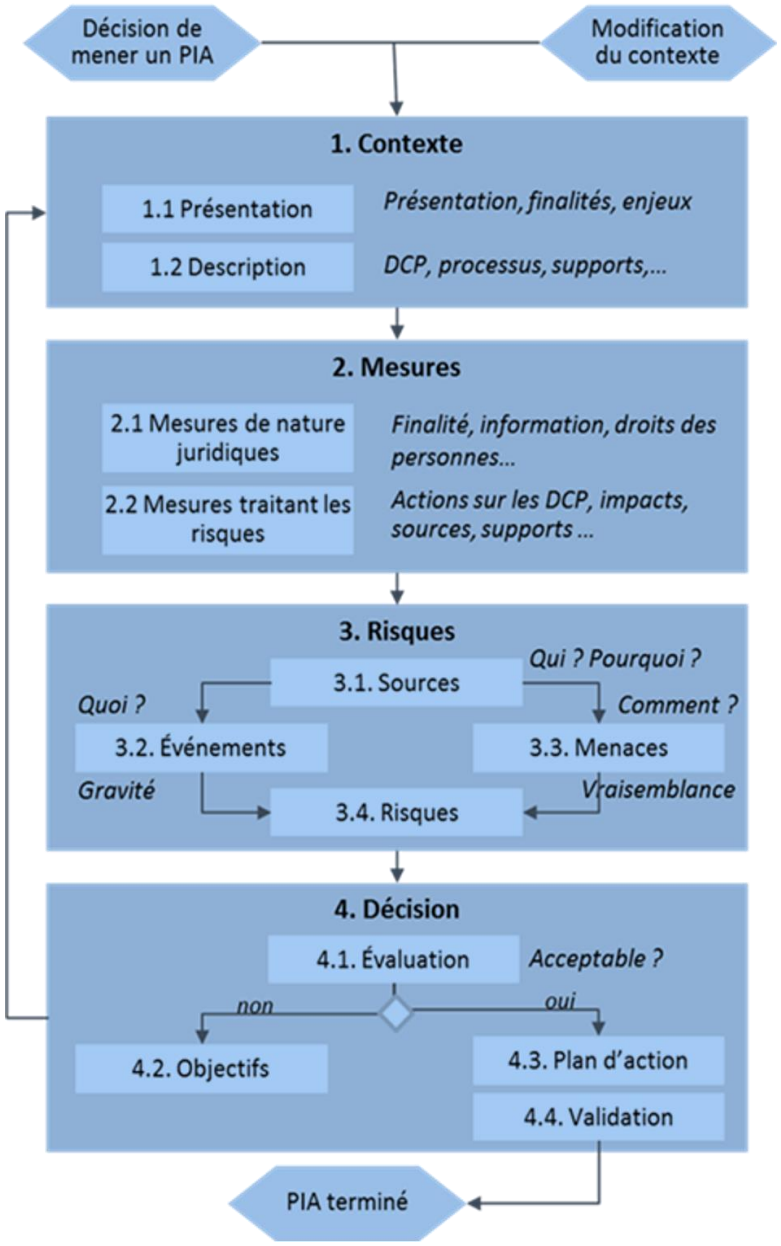
LES PARTIES PRENANTES

Présence

Assurez-vous de la présence de l'ensemble des parties prenantes au moment de l'analyse.

Information

Assurez-vous que les parties prenantes disposent des informations et connaissances nécessaires au moment de l'analyse.



LA MÉTHODE EBIOS

La méthode EBIOS a été adoptée et adaptée au contexte « Informatique et Libertés »

01

Décrire le contexte

Délimiter et décrire le contexte du traitement considéré

02

Identifier les mesures

Analyser les mesures garantissant le respect des principes fondamentaux

03

Apprécier les risques

Vérifier que les risques sur la vie privée liés à la sécurité des données sont correctement traités

04

Prendre une décision

Formaliser la validation de l'AIPD en acceptant les risques résiduels.
En cas de refus il convient de se fixer des objectifs

LE MOMENT EST VENU POUR VOUS D’OBTENIR LA VÉRITÉ, CAR TOUT CELA VOUS L’AVIEZ DÉJÀ ENTENDU

LA VERITE SUR LES PARTIES PRENANTES

Présence

Il est le seul à comprendre l'importance de ce chantier, néanmoins il est souvent esclave du manque d'implication des autres parties prenantes.

Les métiers et le RSSI

La vérité, c'est que les métiers devront répondre à deux questions par AIPD.
Quand au RSSI et/ou le DSI, ils devront à minima recenser avec vous l'ensemble des mesures pour chaque AIPD.

IL Y A 7 RÉPONSES QUE VOUS NE TROUVEREZ PAS DANS LA FICHE DE TRAITEMENT

LES DEUX QUESTIONS POUR LES MÉTIERS

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

Comment se déroule la collecte ? La transformation ? La conservation ? L'utilisation ? Les transferts ? La destruction ?

Quels pourraient-être les principaux impacts sur les personnes concernées si le risque se produisait ?

En cas d'accès illégitime que pourrait-il arriver ?

En cas d'altération ou de destruction quel processus ne pourriez-vous plus assurer ?

Il est probable que les réponses soient souvent les mêmes pour une typologie de personnes concernées. **C'est un facteur récurrent**

Quelles sources de risques pourraient-elles en être à l'origine ?

Les sources de risques sont liées la majeure du temps à votre environnement.

Trouvez-les **c'est un facteur récurrent**.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Le RSSI à toute les réponses, c'est son métier d'être un peu parano.

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Le RSSI sait quelles sont les mesures existantes permettant de répondre aux différents points de contrôle d'EBIOS

Quelles sources de risques Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Le DPO devra répondre à cette question, il mettra la seconde réponse des métiers face aux mesures existantes diminuant la gravité

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Le RSSI devra répondre à cette question, l'objectif est de prendre en compte les mesures existantes diminuant la vraisemblance en fonction des supports concernées.

RAPPEL 1 : LA FORMULE

LA GRAVITE

X

LA VRAISEMBLANCE

=

LE RISQUE

RAPPEL 2 :
APPRÉCIER LES RISQUES

COMMENT APPRÉCIER LES RISQUES ?

Il existe trois démarches d'appréciations possibles des risques :

- Le risque BRUT représente le risque sans aucune mesure
- Le risque NET représente le risque avec les mesures existantes
- Le risque RESIDUEL représente le risque avec des mesures complémentaires planifiées et budgétisées

Le risque INITIAL d'une AIPD est un risque NET

RAPPEL 3 :
LE PLAN D'ACTION EST TOUJOURS POSSIBLE

LES RISQUES RÉSIDUELS SONT ÉLEVÉS

Il existe deux possibilités :

- Refuser et refixer des objectifs *(difficile pour les traitements déjà en production)*
- Planifier et budgétiser des mesures complémentaires

QUE FAIRE SI LES RISQUES RÉSIDUELS RESTENT ÉLEVÉS ?

Le CEPD (ex G29) considère que la consultation est obligatoire quand les risques résiduels demeurent élevés.

[Art 36(1)]

RAPPEL 4 : LES SANCTIONS

QUE RISQUE-T-ON ?

« Amendes administratives pouvant s'élever jusqu'à 10 000 000 € ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu » [art. 83(4)(a)]

DANS QUELS CAS ?

- Quand un PIA n’a pas été mené alors qu’il aurait dû l’être
- Quand un PIA n’a pas été correctement mené et documenté
- Quand la CNIL n’a pas été consultée alors qu’elle aurait dû l’être conformément à l’article 36

QUELLES MESURES CHOISIR POUR DIMINUER LA GRAVITÉ OU LA VRAISEMBLANCE ?

	Accès illégitime	Modification non désirée	Disparition
Gravité	• Respect des durées de conservation • Minimisation • Anonymisation • Pseudonymisation • Chiffrement	• Sauvegarde • Traçabilité	• Sauvegarde • Traçabilité
Vraisemblance	• Sensibilisation du personnel • Cloisonnement des données • Contrôle d'accès logique • Revue régulière des habilitations • Surveillance (paramétrages, contrôles de configurations, surveillance en temps réel...) • Gestion des postes de travail • Lutte contre les codes malveillants (virus, logiciels espions, bombes logicielles...) : • Protection des canaux informatiques (réseaux) : • Contrôle d'accès physique • Sécurité des matériels • Sécurité des documents papier • Sécurité des canaux papier	• Traçabilité • Contrôle d'intégrité • Éloignement des sources de risques (produits dangereux, zones géographiques dangereuses...) • Protection contre les sources de risques non humaines (feu, eau...) • Contrôle d'accès physique	• Traçabilité • Éloignement des sources de risques (produits dangereux, zones géographiques dangereuses...) • Sécurité des matériels • Protection contre les sources de risques non humaines (feu, eau...) • Contrôle d'accès physique

MERCI