

LISTE DES QUESTIONS QUE DOIT SE POSER LE CIL POUR UN PROJET D'ANONYMISATION DE DONNEES

Dans le cadre de ses travaux sur le thème de l'anonymisation de données, le groupe *Référentiels et Labels* de l'AFCDP suggère une liste de points que le Correspondant Informatique & Libertés doit aborder et valider dans le cadre d'un projet d'anonymisation de données.

Le Correspondant Informatique & Libertés peut apporter son aide aussi bien en amont du projet (avis sur le périmètre et sur le processus envisagé, participation au choix de l'outil, recommandations quant à sa mise en œuvre, sensibilisation des personnels, etc.) qu'en aval (contrôles réguliers, vérification du respect des procédures, propositions d'améliorations, etc.). Naturellement, cette démarche s'effectue en pleine coopération avec les fonctions concernées par le projet ; responsable des développements, RSSI, Risk manager, responsable informatique, etc.

Il concoure ainsi à la protection des données personnelles et à la réduction effective du risque qui pèsent sur l'entité et le responsable du traitement.

Les membres du groupe doivent être remercié pour le travail accompli :

- Eric Barbry, Alain Bensoussan Avocats
- Yann le Hegarat, +SELF+
- Bernard Lombardo, Ugap
- Bruno Rasle, Cortina
- Alain Rouffiat, Princeton Softech
- Michel Simion, Compuware
- Gilles Trouessin, Oppida

Ce document est perfectible. Le groupe *Référentiels et Labels* invite les membres de l'AFCDP à faire part de toute remarque et proposition visant à l'améliorer.

On pourra se reporter avec profit au Glossaire « Anonymisation des Données » édité par le même groupe de travail

Arnaud Belleil
Cecurity.com
Administrateur AFCDP

I – Opportunité du projet d’anonymisation

- Existe-t-il des obligations réglementaires à anonymiser les données ?
- Existe-t-il un risque pour l’organisation (de ne pas anonymiser les données) en terme d’image de marque ?
- Existe-t-il un risque pour l’organisation (de ne pas anonymiser les données) en terme d’intelligence économique ?
- Existe-t-il une obligation « Corporate » pour mettre en œuvre un projet d’anonymisation ?
- Le projet concerne-t-il un nouveau traitement ou bien un traitement existant ? Dans ce dernier cas, quelle stratégie de protection des données l’anonymisation est-elle destinée à remplacer/à compléter ?

II – Organisation du projet d’anonymisation

- Le projet a-t-il un caractère d’urgence ? Doit-il impérativement être achevé à une date précise ?
- Ce projet est-il abordé dans sa globalité et non sous le seul angle du choix d’une solution ?
- Qui est responsable du projet d’anonymisation ?
- Quels sont les acteurs impliqués par le projet d’anonymisation au sein de l’organisation (responsable du traitement, RSSI, responsable des études, etc.) ?
- Quel est le périmètre du projet d’anonymisation par rapport aux usages des données (développement, production, tests, formation, archivage, datamining, ...) ?
- Quel est le périmètre du projet d’anonymisation par rapport aux contenus des bases des données (quelles données doivent être anonymisées) ?
- Quels sont les destinataires des données devant faire l’objet d’une anonymisation (profil d’accès, pays hors Union européenne, ...) ?
- Le projet est-il mis en œuvre en coopération avec la CNIL (rôle de conseil) ?
- Le processus d’anonymisation des bases de données est-il formalisé dans un document ?
- Une procédure de contrôle est-elle prévue après la mise en œuvre du processus d’anonymisation des données ? Qui la mènera et selon quel protocole ?
- Au sein du processus d’anonymisation, les différents acteurs sont-ils clairement identifiés, ainsi que sont définis leur rôle et leur objectif respectif ?
- Les différents acteurs du projet ont-ils été formés (exemple : mise en œuvre des stratégies d’anonymisation adéquates) ?
- Une phase préliminaire expérimentale est-elle envisagée afin de valider le processus ?

III – Solution d’anonymisation

- Est-il prévu d’acquérir un progiciel ou de réaliser des développements spécifiques ?
- Le fournisseur de la solution mise en œuvre (ou ses représentants) assure-t-il son rôle de conseil par rapport au projet d’anonymisation ?
- La solution envisagée est-elle adaptée au cadre réglementaire national ?
- Existe-t-il une sécurisation de l’accès à la solution (authentification, traçabilité, etc.) ?
- La solution assure-t-elle une traçabilité des actions ?
- La solution permet-elle d’enregistrer la stratégie d’anonymisation afin de pouvoir la rejouer ultérieurement ?
- La solution est-elle intégrée au système d’information de l’organisation ou utilisée de façon indépendante ?
- Quelles sont les techniques d’anonymisation proposées par la solution ?

La solution dispose-t-elle :

- d’une fonctionnalité d’anonymisation par appauvrissement des données ?
- d’une fonctionnalité d’anonymisation par masquage des données ?
- d’une fonctionnalité d’anonymisation par suppression des données ?
- d’une fonctionnalité d’anonymisation par chiffrement des données ?
- d’une fonctionnalité d’anonymisation par vieillissement des données ?
- d’une fonctionnalité d’anonymisation par génération de données fictives ?
- d’une fonctionnalité d’anonymisation par mélange de données ?
- d’une fonctionnalité d’anonymisation par obfuscation des données ?
- d’une fonctionnalité d’anonymisation par calcul d’empreinte (hachage) ?
- d’une librairie de données fictives ? Si oui, la librairie de données fictives est-elle adaptée au contexte national ?

La solution permet-elle :

- de réaliser une anonymisation partielle de la base de donnée ?
- de mettre en œuvre une stratégie d’anonymisation reposant sur l’association de différentes méthodes ?