COMMENT REALISER UNE EVALUATION D'IMPACT SUR LA VIE PRIVEE (EIVP)

POUR LES DISPOSITIFS RFID ?

Septembre 2013

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

RÉPUBLIQUE FRANÇAISE

SOMMAIRE

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

I. UNE METHODOLOGIE EUROPEENNE

Depuis 2009, la Commission européenne recommande aux potentiels exploitants de RFID d'évaluer l'impact du dispositif RFID qu'ils envisagent de mettre en œuvre sur la vie privée des utilisateurs du dispositif et sur toute personne concernée.

En outre, le 12 janvier 2011, le G29 a validé un cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID)[1].

Ce cadre doit être suivi par les futurs exploitants de RFID afin de réaliser une **étude d'impact sur la vie privée (EIVP** ou Privacy Impact Assessment framework-« *PIA framework* »- en anglais) conforme aux attentes de la Commission européenne et de la CNIL.

L'objectif de cette fiche pratique est de présenter les caractéristiques principales de ce cadre méthodologique, afin d'aider les futurs exploitants qui doivent réaliser une EIVP à mettre à disposition de la CNIL un document clair et synthétique autant qu'il sera précis et complet.

A. PRESENTATION GENERALE DE LA METHODOLOGIE EUROPEENNE

Globalement, il convient de retenir que ce document (de 25 pages) doit permettre au futur exploitant d'évaluer les risques d'atteinte à la vie privée et à leur impact sur les personnes concernées par les applications RFID. Elle conduit à évaluer la vraisemblance de ces risques et à documenter les mesures prises pour y faire face.

La méthodologie à mettre en œuvre pour évaluer l'impact sur la vie privée (EIVP) est présentée en 2 parties.

Dans une **première partie** (12 pages), la notion d'EIVP est explicitée à travers :

- des éléments de définition ;
- des concepts clefs ;
- une présentation de l'impact de l'EIVP sur la redéfinition des procédures internes ;
- une présentation détaillée du processus d'EIVP, qui soit être mené en 3 étapes, à savoir une analyse préalable, une évaluation des risques et un rapport d'EIVP.

[1] Cadre d'évaluation accessible sur http://www.centrenational-rfid.com/docs/users/file/pia-fr.pdf.

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Dans une **seconde partie**, plusieurs annexes proposent des supports de réflexion opérationnelle afin que l'exploitant mette en œuvre une EIVP complète (ou limitée), tels :

- un tableau de synthèse permettant une description de l'application RFID (annexe I) ;
- un tableau de description des objectifs en matière de respect de la vie privée (annexe II) ;
- un tableau de présentation des risques en matière de respect de la vie privée (annexe III) ;
- des exemples de dispositifs de contrôle des applications RFID et de mesures de limitation des risques (annexe IV).

Au moyen de l'ensemble de ces éléments, et du rapport d'EIVP finalement retenu, les futurs exploitants de dispositifs RFID seront à même de respecter une obligation d'information et de transparence vis-à-vis du public, en **rendant publique une politique d'information « *concise, précise et aisément compréhensible* »**.

En effet, cette information doit notamment indiquer l'identité et l'adresse des exploitants, l'objet de l'application, les données traitées mais également un résumé de l'EIVP, ainsi que les risques probables que ces puces peuvent avoir sur la vie privée et les mesures prises pour limiter ces risques.

II. LES 3 ETAPES A SUIVRE POUR REALISER UNE EIVP

A. L'ANALYSE PREALABLE

La première étape de l'EIVP consiste en une **pré-évaluation** du niveau de risque global d'atteinte à la vie privée de l'application RFID . Ce niveau de risque est classé de 0 à 3. Un tel classement permet de déterminer si une EIVP est nécessaire, ainsi que son degré de détail.

Le **niveau 0** concerne les applications RFID qui **ne traitent pas de données à caractère personnel** et qui dont les puces **ne sont pas portées par une personne physique (**ex : identification des pièces de rechange utilisées dans une usine, identification des palettes dans un entrepôt).

Dans un tel cas, compte tenu de l'absence de risque d'atteinte à la vie privée d'une personne, il n'est **pas nécessaire de réaliser d'EIVP**.

Le niveau 1 concerne les applications qui ne traitent pas directement de données à caractère personnel, mais dont les étiquettes RFID peuvent être portées par des personnes physiques (ex : une veste qui contiendrait une étiquette RFID dont la seule utilité est de servir d'antivol ou d'outil pour les inventaires, sans aucun lien entre le numéro de l'étiquette et le fichier client).

Dans un tel cas, seule une **EIVP limitée** doit être réalisée : l'analyse à produire devra être principalement orientée sur les risques liés à la détention éventuelle des puces RFID par des individus.

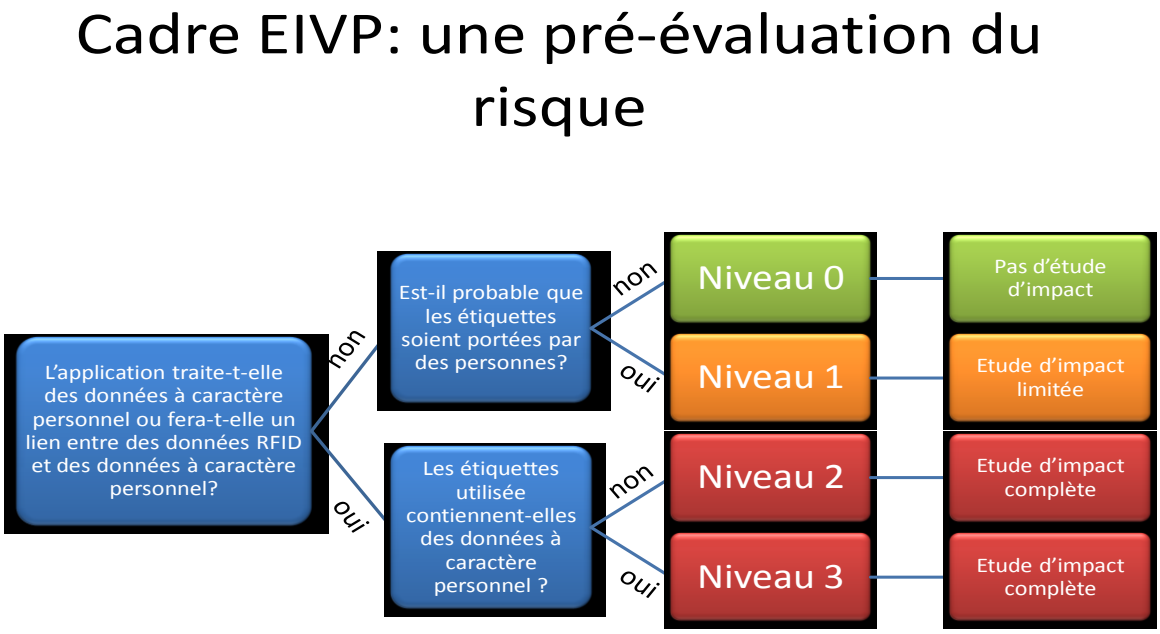
Le **niveau 2** concerne les applications qui **traitent des données à caractère personnel**, mais dont les **étiquettes RFID ne contiennent pas de données identifiantes** (ex : une veste contient une étiquette RFID dont le numéro est relié au fichier client par le biais de la carte de fidélité du client).

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Dans un tel cas, il est nécessaire de réaliser une EIVP complète selon le modèle proposé par la méthodologie présentée dans cette fiche.

Le **niveau 3** concerne les applications qui **traitent directement des données à caractère personnel** - ex : le passe Navigo, qui contient un identifiant de l'individu ainsi que ses 5 derniers points de passage).

Dans ce cas il est également nécessaire de réaliser une **EIVP complète.**



B. LA PHASE D'EVALUATION DES RISQUES

La méthodologie retenue s'appuie sur une approche de **gestion des risques,** la notion de « risque » devant être interprétée au un sens large, notamment concernant la sécurité des données. Cette phase d'évaluation des risques doit être menée à l'appui de l'annexe III.

« En miroir » de l'évaluation de ces risques, doivent être évaluées les mesures de limitation des risques identifiés, dont certains exemples sont fournis en annexe IV de la méthodologie présentée.

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

C. LE RAPPORT D'ETUDE D'IMPACT SUR LA VIE PRIVEE

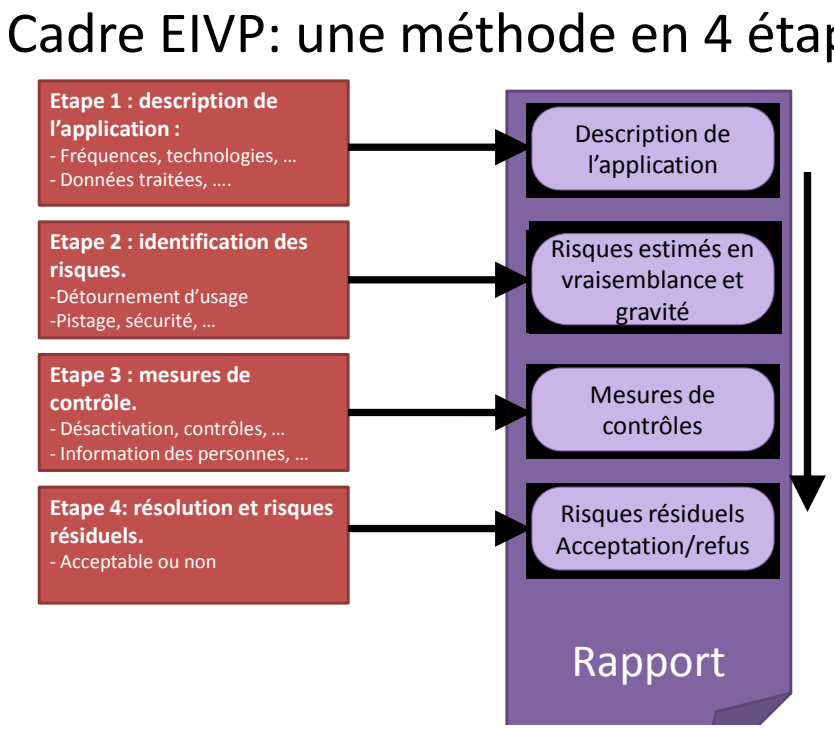
Il s'agit du document présentant de manière synthétique (de 3 à 5 pages selon les dispositifs concernés et les enjeux « Informatique et libertés » à envisager) les risques d'atteinte à la vie privée pour les personnes concernées, les mesures prises pour les minimiser ces risques ou les supprimer.

Il doit comporter **quatre parties** :

- la première partie de l'étude consiste à décrire l'application RFID ;
- la seconde partie permet d'identifier les risques pesant sur la vie privées des personnes concernées, d'évaluer leurs vraisemblance et leur gravité, de détailler les mesures de contrôle et de sécurité mises en œuvre dans l'application RFID décrite ;
- la troisième partie est dédiée aux droits et à l'information des personnes ;
- Enfin, la quatrième et dernière partie de l'étude consiste à conclure sur la possibilité de déployer ou non l'application RFID en l'état des risques résiduels.

Ces quatre parties sont complétées par des annexes destinées à guider le travail d'évaluation d'impact réalisé par l'exploitant, réalisées sur le modèle des annexes de la méthodologie proposée.

NB : L'EIVP identifiera (dans la quatrième partie du document) les modalités de gestion interne de l'ensemble des mesures techniques et organisationnelles retenues (services concernés, personnes habilitées, lignes budgétaires, calendrier de mise en œuvre, fréquence des points d'étape et de bilans).



8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

1. Conseils essentiels pour rédiger une EIVP

- Identifier les risques en matière de vie privée, notamment en matière de traçage des individus par l'exploitant ou par des tiers (susceptibles de disposer de lecteurs RFID).
- Ne pas se limiter à lister les avantages de la mise en œuvre du dispositif.
- Etre « objectif » : il faut prendre du recul par rapport au projet. Idéalement, c'est au CIL que reviendra la mission de rédiger ou bien de finaliser le rapport d'EIVP, ou, à défaut, à la personne en charge de la gestion des risques ou de la conformité.
- Ne pas minimiser les risques afin de ne pas donner l'impression que les motivations du projet, qu'elles soient économiques ou commerciales, l'emportent sur les critiques potentielles.
- Documenter le processus : à un risque donné doit correspondre une mesure corrective donnée.
- Etre conclusif : le dispositif est-il risqué ou non pour les personnes ? Quelles solutions répondent de manière satisfaisante aux risques identifiés ?

2. Existe-t-il des modèles ou illustrations d'EIVP ?

Tout d'abord, il convient de noter que les guides « Gestion des risques Vie privée » partie I et partie II, publiés par la Commission et accessibles sur le site de la CNIL aideront les futurs exploitants de dispositifs RFID à appréhender la notion d'analyse de risques pour la vie privée.

Par ailleurs, plusieurs modèles d'étude d'impact sont accessibles sur le site du « Club EBIOS » (voir sur ce point des exemples d'études de cas)

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00