

Questions relatives au PIA Framework
Cadre général pour l'étude d'impact sur la vie privée et la protection des données des applications RFID

Suite aux Assises de la RFID tenues le 31 mai 2011 au ministère de l'économie, des finances et de l'industrie à Paris, les participants ont posé un certain nombre de questions.

Globalement favorables à la prise en compte des risques liés au respect de la vie privée et aux données à caractère personnel dans les applications RFID, ces derniers ont souhaité quelques éclaircissements suite aux conférences lors des Assises.

Ce qu'il faut faire pour réaliser ce PIA semble clair. En revanche, le timing, l'impact, le contrôle, la protection apportée et l'avantage concurrentiel qu'ils pourraient en tirer méritent d'être abordés plus clairement.

Ce document reprend les questions les plus fréquentes. Les réponses ont été élaborées par le Centre National RFID, la DGCIS et la DG INFSO de la Commission européenne.

Q1	Le PIA a été publié en anglais en janvier et signé a priori fin mars début avril par l'industrie « allemande » ?
R1	<p>Le document : « Privacy and Data Protection Impact Assessment Framework for RFID Applications » a été publié par la Commission européenne le 12 janvier 2011. Une cérémonie de signature s'est tenue à Bruxelles le 6 avril 2011. Le document a été signé par les personnes suivantes : Neelie Kroes, Vice-présidente de la Commission européenne, Jacob Kohnstamm, Chairman Art.29 Data Protection WP, Heinz-Paul Bonn, Vice-president Bitkom, Véronique Corduant, EU Chair EABC, Miguel Lopera, CEO GS1, Jürgen Noack, Advisor EuroCommerce, Paul Skehan, Director European Retail Round Table (ERRT), Eldor Walk, Technical Director AIM Germany, Hudo Helmbrecht, Executive Director ENISA.</p> <p>Il est aujourd'hui traduit en français et disponible sur le site internet du Centre National RFID ainsi qu'à l'adresse suivante : http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm</p>
Q2	L'industrie allemande n'est pas l'industrie française. Sommes-nous dès lors vraiment concernés ?
R2	Le document est européen, il concerne donc l'ensemble des états membres. Il a été approuvé par le groupe de travail de l'article 29 sur la protection des données (donc en France par la CNIL). L'industrie française a été à plusieurs reprises tenue informée de l'avancement des travaux à travers la DGCIS ou le Centre National RFID. Les réactions françaises (trop rares) ont bien évidemment été transmises à Gérald Santucci, chef de l'unité « Réseaux d'entreprise et RFID » à la DG Société de l'information et Médias (INFSO). Les industriels français peuvent désormais contribuer à la mise en œuvre du document travers l'élaboration de modèles sectoriels (<i>templates</i>) destinés à clarifier l'interprétation du cadre général dans divers contexte sectoriels et donc à simplifier le travail de rédaction du rapport de PIA pour des cas d'usage récurrents.

Q3	Est-ce obligatoire ? Si non, quand est-ce que ce sera obligatoire en France ?
R3	<p>Le document sert aux opérateurs RFID à faire en sorte que leur application soit en accord avec la Recommandation européenne du 12 mai 2009. Il n’y a, pour le moment, aucune contrainte légale ou réglementaire européenne ou française.</p> <p>Comme pour toute recommandation, un audit sera mené par la Commission européenne auprès des états membres trois ans après la parution du texte, soit au plus tard en mai 2012. Suivant les résultats de cette enquête, la Commission européenne décidera ou non de passer de l’étape Recommandation à l’étape Directive. Dans ce cas, la future directive devrait être traduite dans le droit français.</p> <p>Il en va de chaque opérateur français de se conformer au mieux à la Recommandation afin de rester dans un cadre plus souple de co-régulation. En tout état de cause, l’application RFID doit être conforme aux directives 95/46/EC, 99/5/EC et 2002/58/EC.</p>
Q4	Quelle durée pour sa mise en place (phase intermédiaire ou de transition – 6 mois par exemple) ?
R4	<p>Dans son avis du 11 février 2011, le groupe de travail de l'article 29 sur la protection des données indique que « le cadre général s'appliquera au plus tard 6 mois après la publication de cet avis », soit en principe à compter de septembre 2011. Il entérine ainsi la disposition finale du cadre général PIA : « Le cadre général PIA prendra effet au plus tard 6 mois après sa publication et son approbation par le groupe de travail de l'article 29 sur la protection des données. » Bien entendu, le temps requis pour une telle étude dépend de la complexité de l’application RFID. Par contre, cette évaluation d’impact sur la vie privée et les données à caractère personnel doit être transmise à la CNIL 6 semaines avant la mise en place opérationnelle de l’application RFID.</p>
Q5	Le PIA n’est pas rétroactif mais quid pour les applications en cours de développement et qui seront en production dans 3 à 6 mois ? (et pour lesquelles le travail correspondant n’a pas été chiffré)
R5	<p>Le document « Cadre général pour l’étude d’impact sur la vie privée et la protection des données des applications RFID » stipule dans sa disposition finale : « Le cadre général prendra effet au plus tard six mois après sa publication et son approbation par le groupe de travail de l'article 29 sur la protection des données. Pour les applications RFID mises en place avant son entrée en vigueur, il ne s'appliquera que lorsque les conditions de présentation d'une nouvelle étude d'impact de l'application RFID sur la vie privée ou d'une étude révisée seront réunies, conformément aux dispositions du cadre général. » Toute nouvelle application RFID doit désormais faire l’objet d’une étude d’impact qui sera transmise au représentant du groupe de l’article 29 du pays concerné (la CNIL pour la France), et cela six semaines avant la mise en œuvre de ladite application (clause n°5 de la Recommandation du 12 mai 2009).</p>

Q6	<p>La « non rétroactivité » n'est-elle pas une prime donnée aux grands groupes, mettant déjà en œuvre des applications RFID et qui seront exonérés d'analyse ?</p> <p>Elle pénalise les plus petites structures où tout reste à faire en matière de RFID, et chez qui les coûts supplémentaires de l'analyse s'ajouteront au ticket d'entrée déjà élevé en matière de RFID.</p>
R6	<p>Qu'ils aient mené ou non une évaluation d'impact sur la vie privée, les opérateurs RFID ayant déployé des applications avant le 12 février 2011 (publication de l'avis du groupe de travail de l'article 29 sur la protection des données), devaient, de fait, se conformer aux Directives 95/46/EC, 99/5/EC et 2002/58/EC.</p> <p>Les opérateurs RFID, issus de PME, sont, a priori, moins structurés pour appréhender les aspects légaux et sociétaux des applications qu'ils mettent en place. Ils ne peuvent cependant pas se dédouaner de leurs obligations. Ils ont aujourd'hui un outil, simple d'utilisation, permettant de garantir leur conformité aux diverses Directives et Recommandations. Ceci permet en réalité de réduire les coûts liés à ces aspects non techniques de la mise en place d'une application RFID. Ceci peut donc être vu comme un avantage par rapport aux sociétés qui ont déjà mis en place des applications RFID et mené une étude d'impact sans l'aide de cet outil. De plus, pour ces sociétés qui n'auraient pas mené d'étude d'impact sur la vie privée et les données à caractère personnel, on peut imaginer que, poussées par celles qui aujourd'hui suivront la Recommandation et par les utilisateurs et citoyens, elles vont mener cette étude a posteriori.</p>
Q7	<p>Une solution non soumise au PIA compte tenu de la non rétroactivité et déployée dans un autre pays européen, mais pas encore en France, sera-t-elle concernée par le PIA lors de son déploiement en France ?</p>
R7	<p>Rappelons tout d'abord qu'aucune application RFID n'est légalement « soumise » à un PIA puisqu'il s'agit d'une recommandation européenne. Elle doit par contre être conforme aux directives 95/46/EC, 99/5/EC et 2002/58/EC.</p> <p>Néanmoins, le cadre général PIA, qui reste un outil d'aide permettant de garantir le respect de la Recommandation de mai 2009, ne prévoit de révision du PIA que lorsque les objectifs de l'application, le matériel utilisé ou le type de données traitées sont modifiés. Il n'y a pas de révision prévue lors d'un élargissement du champ d'application. Une application mise en place dans un des états membres de l'Union européenne qui serait transposée telle quelle dans un autre état membre ne devrait donc pas être soumise à une nouvelle évaluation d'impact. Néanmoins, une copie du PIA d'origine, traduit en français, devrait être transmise à la CNIL lors du déploiement de l'application en France.</p>

Q8	<p>Après entretien avec la CNIL, il s'avère que ce PIA est déclaratif (accusé de réception envoyé par la CNIL) et que son contenu ne sera pas contrôlé.</p> <p>Dès lors, en quoi cela nous protège-t-il ? (responsabilité) et en quoi cela protège-t-il nos clients ?</p>
R8	<p>Il ne faut pas voir le PIA comme un document légal puisqu'il ne s'agit que d'un outil lié à une Recommandation. De plus, il n'est, pour le moment, lié à aucune norme. Son contenu et sa conformité ne peuvent donc pas être officiellement garantis. Néanmoins, de par son positionnement et sa neutralité, le Centre National de référence RFID se propose d'accompagner les opérateurs et pourra valider le contenu du PIA et sa cohérence par rapport à l'application.</p> <p>L'opérateur qui met en place un PIA se dote d'un outil de contrôle de son application RFID vis-à-vis de la protection de la vie privée et des données à caractère personnel. Il a donc tout intérêt à communiquer sur ce point afin de rassurer les utilisateurs, les citoyens et ses clients. Cela lui permet d'avoir les réponses aux inquiétudes que pourraient susciter son application.</p> <p>En cas de manquement à ses obligations légales, l'opérateur pourrait se voir poursuivi et, au-delà des peines encourues, verrait son image de marque et sa crédibilité largement mises à mal. A ce sujet, une étude menée par le CNRFID dans le cadre de la thèse d'Anne-Maël Goulvestre est disponible sur le site du Centre National.</p>
Q9	<p>Quel risque si ce PIA n'est pas réalisé ?</p>
R9	<p>Légalement aucun. La seule chose obligatoire est la conformité de l'application aux directives 95/46/EC, 99/5/EC et 2002/58/EC. L'opérateur n'encourt de poursuites judiciaires que si ces dernières ne sont pas respectées. A ce titre, il faut savoir que la Recommandation du 12 mai 2009, issue d'une démarche de corégulation impliquant la Commission européenne, le groupe de travail de l'article 29 sur la protection des données, l'industrie et la société civile, constitue l'interprétation juridique faite des directives communautaires susnommées par rapport au cas particulier de la RFID. Le PIA permet donc à l'opérateur de se poser les bonnes questions lors du développement de son application.</p> <p>Par ailleurs, en vertu du mandat M/436 donné par la Commission européenne aux organismes européens de normalisation (CEN, CENELEC, ETSI), le cadre général PIA a vocation à devenir une Norme Européenne ("EN") à l'horizon 2013.</p> <p>Enfin, lorsqu'en 2014, soit trois ans après la publication de son avis, le groupe de travail de l'article 29 sur la protection des données dressera le bilan de la mise en œuvre du cadre général PIA, il évaluera le degré de réalisation des PIA et pourrait être conduit, en cas d'insuffisance, à préconiser la mise en œuvre d'une directive.</p>

Q10	La réalisation de ce PIA donne-t-il une garantie à l'intégrateur ?
R10	La notion d'intégrateur n'est pas définie dans la Recommandation de mai 2009 ou dans le cadre général PIA. On parle d'opérateur : « <i>celui qui détermine les finalités et les moyens de faire tourner une application, y compris les contrôleurs de données personnelles utilisant une application RFID</i> ». L'intégrateur RFID proposant une solution technique n'est donc pas, à proprement parler, responsable de son utilisation. Il doit néanmoins, par ses compétences, permettre à l'opérateur d'appréhender les possibilités de la technologie et l'aider à évaluer les risques et mettre en place les mesures nécessaires.
Q11	La réalisation de ce PIA donne-t-il une garantie aux clients ?
R11	Si on entend par client l'opérateur de l'application RFID, le PIA lui permet de s'assurer que tout a été mis en œuvre pour minimiser les risques de son application sur la vie privée et les données à caractère personnel. Il assure donc qu'il a lui-même pris les mesures nécessaires ou qu'il a fait prendre les mesures nécessaires aux divers fournisseurs de solution RFID (fournisseurs de matériel, software ou intégrateurs). Si le client est le citoyen consommateur, le PIA mis en œuvre par l'opérateur RFID lui assure que sa vie privée n'est pas menacée et que ses données à caractère personnel ne pourront pas être utilisées à son insu ou détournées.