Cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données

11 février 2011

TABLE DES MATIÈRES

1. Introduction

La Commission européenne (ci-après dénommée «la Commission») a émis, le 12 mai 2009, une recommandation sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence (ci après dénommée «la recommandation RFID»). En vertu de cette recommandation, un cadre d'évaluation de l'impact des applications RFID sur les données à caractère personnel et la vie privée, mis au point par les entreprises, doit être soumis pour approbation au groupe de travail «article 29» sur la protection des données. Cette évaluation est couramment appelée «évaluation de l'impact sur la vie privée» (EIVP). Le cadre d'évaluation de l'impact des applications RFID sur la vie privée (ci-après dénommé «le cadre») constitue une réponse à cette exigence.

Entreprendre des EIVP concernant les applications RFID présente de nombreux avantages, parmi lesquels celui d'aider les exploitants d'applications RFID à:

- assurer le respect de la législation et des réglementations relatives au respect de la vie privée et à la protection des données;
- gérer les risques pesant sur leur organisation et sur les utilisateurs des applications RFID (du point de vue tant du respect de la vie privée et de la protection des données que de la perception du public et de la confiance des consommateurs); et
- assurer que les applications RFID profitent au plus grand nombre tout en évaluant le respect de la vie privée, en apportant un soin particulier à la conception dès les premières étapes de l'élaboration du cahier des charges ou du processus de développement.

Le processus d'EIVP se fonde sur une approche de la gestion des risques en matière de respect de la vie privée et de protection des données qui est axée essentiellement sur la mise en œuvre de la recommandation RFID de l'Union européenne et qui est conforme aux meilleures pratiques et au cadre juridique de l'Union.

Il est conçu de manière à aider les exploitants d'applications RFID à détecter les risques pour la vie privée associés à une application RFID, à évaluer leur probabilité et à documenter les mesures prises pour y faire face. De tels impacts (s'ils existent) peuvent varier sensiblement selon que l'application RFID traite ou ne traite pas de données à caractère personnel. Le cadre d'EIVP fournit aux exploitants d'applications RFID des orientations concernant les méthodes d'évaluation des risques; il leur propose notamment des mesures appropriées pour limiter de manière efficace, concrète et proportionnée tout impact probable sur la vie privée ou la protection des données.

Enfin, le cadre d'EIVP est suffisamment général pour couvrir toutes les applications RFID, tout en permettant de traiter les particularités et les spécificités au niveau du secteur ou de l'application.

Le cadre d'EIVP s'inscrit dans le contexte d'autres normes de garantie de l'information, de gestion des données et d'exploitation qui favorisent une bonne gouvernance en matière de données pour les applications RFID et autres. Le cadre actuel pourrait servir de base au développement de modèles d'EIVP consacrés spécifiquement à une industrie, à un secteur et/ou à une application en particulier. Comme tout document théorique, le cadre d'EIVP pourrait nécessiter une clarification des termes utilisés et la définition d'orientations en matière de pratiques, qui devraient se fonder sur des expériences concrètes et qui pourraient faciliter sa mise en œuvre.

1.1. Concepts clés

Plusieurs concepts clés utilisés dans le cadre méritent d'être décrits. La ***RFID*** est une technologie qui utilise les ondes électromagnétiques pour communiquer avec des étiquettes RFID et qui permet de lire les numéros d'identification uniques de ces étiquettes ou, éventuellement, d'autres informations qui y sont stockées. Les ***étiquettes RFID*** sont généralement de petite taille. Elles peuvent revêtir de nombreuses formes, mais se composent souvent d'une mémoire électronique, qui peut être lue et éventuellement éditée, et d'antennes. Les ***lecteurs RFID*** sont utilisés pour lire l'information inscrite sur les étiquettes RFID.

Les ***applications RFID*** traitent les informations issues de l'interaction entre les étiquettes RFID et les lecteurs RFID. Elles sont gérées par un ou plusieurs ***exploitants d'application RFID*** et reposent sur des systèmes dorsaux et des infrastructures de communication en réseau. Si l'exploitant d'une application RFID procède à des déterminations liées à la collecte ou à l'utilisation de données à caractère personnel, son rôle peut être similaire à celui du responsable du traitement de données tel que défini dans la directive 95/46/CE; il serait alors décrit comme la personne physique ou morale, l'organisme public, l'agence ou tout autre organe qui, seul ou avec d'autres, définit la finalité et les modalités de l'exploitation d'une application RFID ayant des répercussions sur le plan des informations à caractère personnel.

La terminologie suivante est utilisée dans le contexte de la technologie RFID:

- une ***évaluation de l'impact sur la vie privée (EIVP)*** est un processus impliquant un travail conscient et systématique d'évaluation des effets d'une certaine application RFID sur le respect de la vie privée et la protection des données, entrepris en vue de prendre les mesures qui s'imposent pour prévenir ou à tout le moins réduire au maximum ces impacts;
- le ***cadre*** détermine les objectifs des EIVP portant sur des applications RFID, les composants de ces applications à prendre en considération lors des EIVP ainsi que la structure et la teneur communes des rapports d'EIVP relatifs à des applications RFID;
- le ***rapport d'EIVP*** est le document établi au terme du processus d'EIVP et transmis aux autorités compétentes. Les informations exclusives et sensibles en matière de sûreté peuvent être retirées des rapports d'EIVP avant leur diffusion à l'extérieur (par exemple auprès des autorités compétentes) pour autant qu'elles ne concernent pas spécifiquement les implications sur le respect de la vie privée et la protection des données. Le mode de diffusion des EIVP (par exemple sur demande ou non) sera déterminé par les États membres. L'utilisation de catégories spéciales de données pourra notamment être prise en considération, tout comme d'autres facteurs tels que la présence d'un délégué à la protection des données;
- des ***modèles d'EIVP*** pourront être élaborés sur la base du cadre, afin de fournir des formats spécifiques à une industrie, une application ou autre qui pourront être utilisés dans le cadre des EIVP et des rapports d'EIVP qui en résultent.

Avec d'autres, tels qu'***utilisateurs*** ou ***personnes***, ces termes et expressions sont également définis à l'annexe B: «Glossaire» aux fins du présent cadre d'EIVP. Certains termes provenant de la directive 95/46/CE relatifs à la protection des données y sont également inclus pour référence.

L'exécution et la transmission des EIVP s'ajoutent le cas échéant aux autres obligations potentielles qui incombent aux exploitants d'applications RFID au titre de certaines lois, réglementations et autres accords contraignants.

1.2. Procédures internes

Pour soutenir l'exécution des EIVP, les exploitants d'applications RFID doivent disposer de leurs propres procédures internes, telles que celles présentées ci-dessous:

- la *planification du processus d'EIVP*, afin de disposer de suffisamment de temps pour apporter tous les ajustements nécessaires à l'application RFID et pour transmettre le rapport d'EIVP aux autorités compétentes au moins six semaines avant le déploiement;
- l'*évaluation interne du processus d'EIVP (y compris l'analyse préalable) et des rapports d'EIVP*, de manière à assurer la cohérence avec le reste de la documentation relative à l'application RFID, dont les informations relatives au système, les informations relatives au produit et les exemples de conditionnement du produit et d'utilisation des étiquettes RFID. L'évaluation interne doit permettre un suivi des informations obtenues, de manière à pouvoir traiter tout impact constaté après la mise en œuvre de l'application et à pouvoir adapter les résultats des précédentes EIVP;
- la *compilation des pièces justificatives* (résultats des contrôles de sécurité, projets de dispositifs de contrôle, copies des notifications, etc.) démontrant que l'exploitant de l'application RFID a rempli toutes les obligations qui lui incombent;
- la *désignation, au sein de l'organisation, des personnes habilitées et des fonctions autorisant à entreprendre certaines actions* lors du processus d'EIVP (par exemple, réalisation de l'analyse préalable, rédaction du rapport d'EIVP, signature du rapport d'EIVP, conservation des documents appropriés, et toute répartition des tâches pour ces fonctions);
- la *définition de critères* cohérents par rapport au cadre et à tout modèle d'EIVP correspondant *concernant la manière de déterminer et d'attester qu'une application est prête à être déployée ou pas*;
- la garantie d'une *prise en considération/identification* des *facteurs nécessitant de rédiger un nouveau rapport d'EIVP ou de modifier un rapport existant*. Les critères à retenir devraient inclure: des changements significatifs au niveau de l'application RFID, tels que des changements matériels allant au-delà des objectifs originaux (par ex. objectifs secondaires); les types d'informations traités; les utilisations des informations qui affaiblissent les contrôles mis en place; une violation inattendue des données à caractère personnel[1] ayant un impact déterminant et qui ne faisait pas partie des risques résiduels de l'application mis en évidence par la première EIVP; la définition d'une période d'examen régulier; la réponse à une enquête ou un retour d'informations substantiel ou significatif provenant d'acteurs internes ou externes; ou des modifications technologiques significatives ayant une incidence pour l'application RFID concernée sur le plan du respect de la vie privée et de la protection des données. Les changements matériels qui limiteraient l'étendue de la collecte d'informations ou le champ d'application de l'instrument n'entraînent pas en soi l'obligation d'actualiser l'EIVP. Tout au long du cycle de vie de l'application RFID, il convient de rédiger un nouveau rapport d'EIVP ou d'actualiser le rapport existant si l'application RFID change de niveau, comme décrit dans la section «Analyse préalable»;
- *consultation des parties prenantes*: les avis et les retours d'informations des parties prenantes concernant l'application RFID évaluée devraient être dûment pris en considération lors de l'analyse des préoccupations et des risques potentiels entreprise dans le cadre de l'EIVP. Les consultations devraient être adaptées à

[1] Dans ce cas, la définition qui s'applique est celle de la directive 2009/136/CE modifiant la directive 2002/58 - voir page 29: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:FR:PDF.

l'étendue, au champ d'application, à la nature et au niveau de l'application RFID concernée. Dans les entreprises, des personnes sont désignées pour contrôler et assurer la confidentialité au sein de l'entreprise ou du service. Elles apportent une contribution essentielle au processus d'EIVP dans la mesure où elles participent aux applications RFID spécifiques ou à leur suivi. Les travailleurs maîtrisant les disciplines techniques, commerciales et autres peuvent également se révéler indispensables au processus selon la nature de l'application RFID et leur relation avec celle-ci. Les exploitants d'applications RFID peuvent disposer de mécanismes de consultation par lesquels les intervenants extérieurs, qu'il s'agisse de personnes physiques, d'organisations ou d'autorités, peuvent interagir avec eux et leur fournir un retour d'informations. Dans la mesure où la situation l'exige, l'exploitant d'une application RFID devrait recourir à des mécanismes de consultation pour bénéficier de la contribution des groupes représentant les personnes sur la vie privée desquelles les propositions auront un impact direct, telles que ses employés et ses clients.

2. Le processus d'EIVP

La finalité du cadre est de fournir aux exploitants d'applications RFID des orientations concernant la réalisation d'EIVP pour certaines applications RFID, comme le prévoit la recommandation, et de définir une structure et des catégories de contenu communes pour les rapports dans lesquels les résultats de ces EIVP doivent être consignés. En outre, puisque, dans certains secteurs, de nombreux exploitants d'applications RFID pourraient être intéressés par des applications RFID identiques ou similaires, le cadre pose les jalons du développement de modèles EIVP spécifiques à certaines applications ou à certains secteurs industriels. Les modèles d'EIVP peuvent aider ces secteurs à réaliser des EIVP et à rédiger les rapports correspondants de manière plus efficace pour ces applications RFID similaires[2]. Des applications RFID communes pouvant être proposées dans un certain nombre d'États membres, le cadre est conçu de manière à harmoniser les exigences imposées aux exploitants d'applications RFID dans le respect des législations, réglementations, meilleures pratiques et autres accords contraignants en vigueur dans ces pays.

Le cadre traite du processus d'exécution des EIVP relatives aux applications RFID préalablement au déploiement et précise le champ d'application des rapports d'EIVP qui en résultent[3].

Les exploitants d'applications RFID sont tenus d'organiser une EIVP pour chaque application RFID qu'ils exploitent. S'ils déploient plusieurs applications RFID associées (éventuellement dans le même contexte ou sur le même site), ils peuvent rédiger un seul rapport d'EIVP, pour autant que les limites des applications et les différences entre ces dernières y soient explicitement décrites. S'ils réutilisent une application RFID de la même manière pour une série de produits, services ou processus, les exploitants d'applications RFID peuvent établir un seul rapport d'EIVP pour l'ensemble des produits, services ou processus similaires (exemple: un constructeur automobile déployant les mêmes dispositifs antivol dans tous ses véhicules et dans les mêmes conditions de service). L'exécution et la transmission des EIVP s'ajoutent le cas échéant aux autres obligations

[2] Le concept de reconnaissance mutuelle ou multiple à l'échelle d'entités et de secteurs pour le déploiement d'applications RFID préalablement approuvées devrait être exploré.

[3] Point 5, paragraphe a), de la recommandation de la Commission européenne de mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, C(2009) 3200 final.

potentielles qui incombent aux exploitants d'applications RFID au titre de certaines lois, réglementations et autres accords contraignants.

Le processus d'EIVP se déroule en deux phases:

1. la **phase d'analyse préalable**: l'exploitant d'application RFID suit les étapes décrites dans cette section pour déterminer:

   a) si une EIVP de son application RFID s'impose ou pas; et

   b) s'il convient d'opter pour une EIVP complète ou limitée.

2. la **phase d'évaluation des risques**: elle définit les critères et les éléments à prendre en considération dans le cadre des EIVP complètes et limitées.

2.1. Phase d'analyse préalable

Préalablement à la conduite d'une EIVP relative à une certaine application, chaque organisation doit comprendre comment mettre en œuvre un tel processus en fonction de la nature et du caractère sensible des données traitées, de la nature et du type de traitement ou de gestion des informations qu'il entreprend ainsi que du type de l'application RFID en question. Pour les organisations qui auraient déjà engagé des procédures d'évaluation des risques en matière de respect de la vie privée pour d'autres applications, les critères de classification et les différentes phases du processus devraient les aider à établir une correspondance entre leurs processus d'EIVP existants et le présent cadre.

Pour réaliser l'évaluation préalable, un exploitant d'application RFID doit parcourir l'arbre de décision présenté au schéma 1. Celui-ci l'aidera à déterminer si et dans quelle mesure une EIVP s'impose pour l'application RFID concernée.

Le résultat obtenu durant la phase d'analyse préalable aide à déterminer le niveau de détail requis pour l'évaluation des risques (par exemple: EIVP complète ou limitée).

L'analyse préalable doit être consignée et être communiquée sur demande aux autorités chargées de la protection des données. Pour plus d'informations concernant les éléments à consigner, consulter l'annexe I.

EIVP complète

Une EIVP complète s'impose pour les applications définies comme étant de niveau 2 ou de niveau 3 lors de la phase d'analyse préalable décrite à la section 2.1. Les applications nécessitant une EIVP complète sont par exemple celles traitant des informations à caractère personnel (niveau 2) ou celles dont l'étiquette RFID contient des données à caractère personnel (niveau 3). Si le niveau 2 et le niveau 3 nécessitent tous les deux une EIVP complète, ils correspondent à des environnements de risque différents et impliquent donc des stratégies différentes d'atténuation des risques. Ainsi, les applications de niveau 2 peuvent être équipées de dispositifs de contrôle destinés à protéger les données d'arrière-plan, tandis que les applications de niveau 3 peuvent être munies de dispositifs de contrôle destinés à protéger à la fois les données d'arrière-plan et les données des étiquettes. Sur la base des expériences accumulées, l'industrie peut affiner plus encore cette classification en niveaux et la manière dont elle adapte le processus d'EIVP en conséquence. Puisque l'application traite des données à caractère personnel, une évaluation des risques extrêmement poussée (évaluation complète) s'impose pour garantir la pertinence des mesures de limitation des risques. Elle aidera l'exploitant de l'application RFID à identifier les risques pertinents et à mettre en place des contrôles adaptés. Dans ce contexte, les

exploitants devraient également évaluer si les informations contenues dans l'étiquette RFID sont susceptibles d'être utilisées au-delà de leur finalité de départ ou de l'utilisation qui pouvait en être faite dans l'esprit de la personne concernée, en particulier si elles sont susceptibles d'être utilisées pour traiter des données à caractère personnel ou pour établir un lien avec de telles données, et déterminer si une nouvelle analyse EIVP se justifie ou s'il convient de recourir à d'autres dispositifs de contrôle afin de limiter les risques.

EIVP limitée

Les EIVP limitées suivent le même schéma que les EIVP complètes mais, en raison du profil de risque plus faible, la portée et le niveau de détail de l'enquête et du rapport qu'elles impliquent sont plus limités. Les EIVP limitées se justifient pour les applications de niveau 1. Si une EIVP limitée suit un schéma similaire à celui d'une EIVP complète, les contrôles requis et les éléments à consigner en conséquence dans le rapport d'EIVP sont simplifiés du fait que les risques inhérents à une application de niveau 1 sont moindres que ceux d'une application de niveau 2 ou 3.

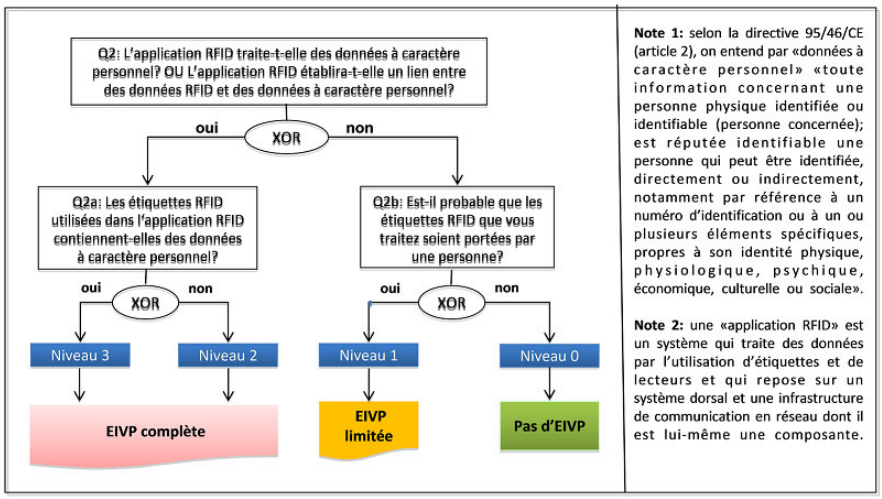


Schéma 1: arbre de décision concernant l'opportunité de mener une EIVP et le niveau de détail à lui donner

2.2. Phase d'évaluation des risques

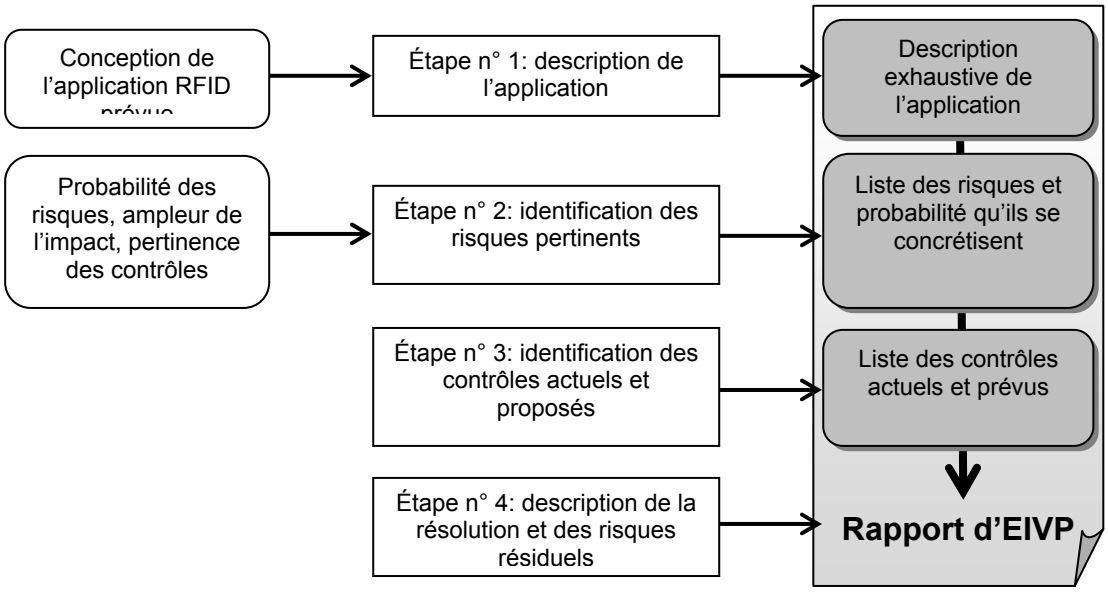
Une évaluation des risques sert à déterminer – idéalement au début du développement d'un système – quels sont les risques que fait peser une application RFID sur la vie privée et à décrire comment ces risques sont *préventivement* limités au moyen de contrôles techniques et organisationnels. Une EIVP joue ainsi un rôle important en matière de respect des dispositions juridiques relatives à la vie privée (directive 95/46/CE) et sert à mesurer l'efficacité des procédures de limitation des risques. Pour économiser du temps et de l'argent, il est recommandé de procéder à cette phase d'évaluation des risques bien avant d'arrêter les décisions définitives relatives à l'architecture d'une application RFID, de sorte que les stratégies techniques d'atténuation des risques pesant sur la vie privée puissent être intégrées à la conception du système plutôt que de venir s'y «greffer» par la suite.

Un processus d'évaluation des risques commence généralement par une analyse des risques inhérents à une application RFID sous l'angle de leur probabilité et de l'ampleur de

leurs conséquences. Il est recommandé aux exploitants d'applications RFID d'utiliser les objectifs en matière de respect de la vie privée définis dans la directive européenne comme points de départ de leur évaluation des risques (cf. annexe II). Les risques pour la vie privée pourraient être élevés en raison de possibles actes de malveillance visant la mise en œuvre de l'application RFID ou de par l'absence de contrôles portant sur le respect de la vie privée au niveau de l'organisation ou de l'environnement. Ils pourraient aussi être limités, simplement parce qu'ils sont peu probables dans l'environnement ou l'organisation concerné ou parce que la configuration de l'application RFID est déjà extrêmement favorable au respect de la vie privée. Le processus d'EIVP doit permettre d'envisager tous les risques potentiels, puis de réfléchir à leur ampleur, à leur probabilité et aux possibilités de les atténuer. Cette réflexion débouche sur l'identification des risques pour la vie privée qui doivent réellement être pris en considération pour le déploiement d'une application RFID au niveau de l'organisation et qui doivent être limités grâce à des contrôles concrets.

Le processus d'EIVP (tel que présenté au schéma 2) exige de l'exploitant d'une application RFID qu'il:

1. décrive l'application RFID;
2. détermine et explique point par point en quoi l'application RFID examinée pourrait constituer une menace pour la vie privée et évalue l'ampleur et la probabilité de ces risques;
3. décrive les contrôles techniques et organisationnels actuels et envisagés destinés à limiter les risques décelés; et
4. présente la résolution (résultats de l'analyse) relative à l'application.



Étape n° 1: description de l'application

La description de l'application doit être une description complète et détaillée de l'application, de son environnement et des limites du système. Elle porte notamment sur la conception de l'application, sur ses interfaces adjacentes avec d'autres systèmes et sur les flux d'informations. Pour qu'ils puissent être visualisés, il est recommandé de représenter ces flux sous forme de diagrammes montrant le traitement des données primaires et secondaires. La structuration des données doit également être décrite, afin que les liens potentiels puissent être analysés. L'annexe I résume les éléments qui caractérisent une application RFID aux fins d'une EIVP.

Il est également recommandé de fournir des informations concernant l'environnement opérationnel et stratégique de l'application. Celles-ci peuvent porter sur les objectifs du système dans l'immédiat et à plus long terme, les différents acteurs de la collecte d'informations, les exigences relatives aux fonctions et l'ensemble des utilisateurs potentiels. Elles peuvent également inclure une description de l'architecture de l'application RFID et des flux de données (et notamment des interfaces avec les systèmes externes susceptibles de traiter des données à caractère personnel).

Étape n° 2: identification des risques

Cette étape doit permettre d'identifier les conditions susceptibles de menacer ou de compromettre la confidentialité des données à caractère personnel, en se basant sur la directive de l'Union européenne pour déterminer les principaux objectifs à atteindre en matière de respect de la vie privée. Les risques peuvent être liés aux composants de l'application RFID, à son fonctionnement (systèmes de collecte, de stockage et de traitement) et à l'environnement de partage et de traitement des données dans lequel elle s'inscrit.

Une liste des risques potentiels en matière de vie privée est présentée à l'annexe III. Elle sert de support à l'identification systématique des risques potentiels pesant sur les objectifs définis dans la directive européenne (annexe II).

Une EIVP nécessite d'identifier les risques, mais aussi de les quantifier de manière relative. Un exploitant d'application RFID devrait déterminer, compte tenu des principes de proportionnalité, la *probabilité* de voir se concrétiser les risques pour la vie privée dans des conditions raisonnables. Les risques peuvent provenir de l'application RFID elle-même et, dans certains cas, de l'extérieur. Ils peuvent résulter tant des utilisations probables de l'information que des usages abusifs qui pourraient en être faits, notamment si les étiquettes RFID utilisées dans l'application RFID restent opérationnelles une fois en la possession de personnes.

L'évaluation des risques nécessite d'évaluer les risques applicables du point de vue de la protection de la vie privée. L'exploitant de l'application RFID devrait prendre en considération:

1. l'importance d'un risque et la probabilité qu'il se concrétise;
2. l'ampleur de l'impact à prévoir si ce risque devait se concrétiser.

Le niveau de risque découlant de cette évaluation peut ensuite être défini comme faible, moyen ou élevé.

Un risque largement évoqué est celui que les étiquettes RFID puissent être utilisées pour établir le profil d'individus et/ou les suivre à la trace. Dans un tel cas de figure, les informations de l'étiquette RFID – et notamment son ou ses identifiants – seraient utilisées

pour retrouver l'identité d'un individu. Les détaillants qui transmettent des étiquettes RFID à leurs clients sans les désactiver ou les retirer automatiquement lors du passage en caisse *pourraient* involontairement faire naître un tel risque. Une question fondamentale est cependant de savoir si ce risque est probable et s'il constitue ou pas, concrètement, un risque *inévitable*. En vertu du point 11 de la recommandation RFID, les détaillants doivent désactiver ou retirer, au point de vente, les étiquettes de leur application à moins que les consommateurs, après avoir pris connaissance de la politique d'information conformément aux dispositions du présent cadre, acceptent que les étiquettes restent opérationnelles. Conformément au point 12 de cette recommandation, ils ne sont pas tenus de désactiver ou de retirer les étiquettes si le rapport d'EIVP établit que les étiquettes utilisées dans une application de détail et restant opérationnelles au-delà du point de vente ne présentent pas de risque probable pour la vie privée ou la protection des données à caractère personnel. Par désactivation des étiquettes, on entend tout processus qui interrompt les interactions d'une étiquette avec son environnement et qui n'exige pas de participation active du consommateur.

Les modèles spécifiques à certains secteurs qui seront développés au fil du temps sur la base du présent cadre pour être utilisés dans différentes industries devraient fournir un support plus précis pour l'identification des risques.

Étape n° 3: identification des dispositifs de contrôle et recommandations en la matière

Cette étape doit permettre d'analyser les dispositifs de contrôle installés ou planifiés afin de réduire au maximum, de limiter ou d'éliminer les risques pour la vie privée qui ont été recensés.

Ces dispositifs peuvent être de nature technique ou non technique. Les dispositifs de contrôle techniques sont intégrés à l'application à la suite de choix de conception ou de politiques pouvant être mises en œuvre sur le plan technique. Il peut s'agir de paramètres par défaut, de mécanismes d'authentification et de méthodes de cryptage. Les dispositifs de contrôle non techniques portent quant à eux sur la gestion et le déroulement des opérations; il s'agit par exemple de procédures opérationnelles. Les dispositifs de contrôle peuvent être axés sur la prévention ou sur la détection. Les premiers préviennent les tentatives d'intrusion, les seconds déclenchent l'alerte en cas d'intrusion ou de tentative d'intrusion.

Il existe également des contrôles «naturels» créés par l'environnement. Ainsi, en l'absence de lecteur capable de suivre à la trace des produits ou des individus (du fait que la présence d'un tel lecteur ne se justifie pas d'un point de vue commercial), les risques sont naturellement inexistants (ou à tout le moins peu probables).

Les risques décelés et le niveau de risque auquel ils correspondent doivent servir à déterminer quels sont les dispositifs de contrôle pertinents et, dès lors, quels sont ceux qu'il convient d'utiliser. Le dossier d'EIVP doit expliquer en quoi les dispositifs de contrôle sont associés aux différents risques et décrire comment ces mesures de limitation des risques pourront entraîner un niveau de risque acceptable.

L'annexe IV contient des exemples de dispositifs de contrôle.

Étape n° 4: présentation de la résolution et des risques résiduels

Une fois achevée l'évaluation des risques, la résolution finale relative à l'application doit être consignée dans le rapport d'EIVP, accompagnée de toute remarque additionnelle concernant les risques, les dispositifs de contrôle et les risques résiduels.

- L’utilisation d’une application RFID est approuvée au terme du processus d’EIVP, lorsque les risques ont été identifiés et que les mesures adéquates pour les limiter ont été adoptées, de manière à garantir que tout risque résiduel significatif a été écarté et, ainsi, à assurer la conformité de l’application, et lorsque les procédures de suivi interne appropriées ont été mises en place et que les autorisations adéquates ont été délivrées.

- Lorsque l’utilisation d’une application RFID n’est pas approuvée en l’état, elle ne pourra faire l'objet d'une nouvelle demande d'autorisation qu'après qu'un plan d'action correcteur spécifique aura été élaboré et qu'une nouvelle évaluation de l'impact sur la vie privée aura été entreprise afin de déterminer si l'application peut désormais être approuvée.

La résolution doit être accompagnée des informations suivantes:

- nom du signataire de la résolution;
- titre de la personne;
- date de la résolution.

Rapport d’EIVP

Les EIVP sont des processus internes portant sur des informations sensibles pouvant avoir des implications en matière de sécurité et sur des informations potentiellement confidentielles et exclusives de l’entreprise relatives à certains produits et processus. Cela étant, un rapport d’EIVP devrait généralement inclure:

1. la description de l’application RFID, comme exposé à l’ANNEXE I;

2. la description des quatre étapes susmentionnées.

Le rapport d’EIVP signé contenant une résolution approuvée doit être transmis au responsable de l’entreprise chargé de la sécurité/de la confidentialité des données, conformément aux procédures internes de l’exploitant d’application RFID. Il est communiqué sans préjudice des obligations de la directive 95/46/CE applicables aux responsables du traitement de données, et notamment l’obligation indépendante de notification à l’autorité compétente énoncée à la section IX de cette directive.

3. Disposition finale

Le cadre d’EIVP prendra effet au plus tard six mois après sa publication et son approbation par le groupe de travail «article 29» sur la protection des données. Pour les applications RFID en place avant son entrée en vigueur, il ne s'appliquera que quand les conditions de présentation d'une nouvelle EIVP ou d'une EIVP révisée seront réunies, conformément aux dispositions du cadre d'EIVP.

ANNEXE I – *Description de l'application RFID*

L'exploitant d'application RFID doit intégrer, le cas échéant, les informations ci-dessous au rapport d'EIVP.

Exploitant d'application RFID	• Nom et localisation de l'entité juridique • Personne ou bureau responsable du respect du calendrier d'EIVP • Point(s) de contact et marche à suivre pour poser des questions à l'exploitant
Présentation générale de l'application RFID	• Nom de l'application RFID • Objectif(s) de la/des application(s) RFID • Scénarios d'utilisation de base de l'application RFID • Composants de l'application RFID et technologies utilisées (c'est-à-dire fréquences, etc.) • Portée géographique de l'application RFID • Types d'utilisateurs/de personnes sur lesquels l'application RFID a une incidence • Accès individuel et contrôle
Numéro du rapport d'EIVP	• Numéro de version du rapport d'EIVP (permettant de reconnaître une nouvelle EIVP ou de simples modifications mineures) • Date de la dernière modification apportée au rapport d'EIVP
Traitement des données RFID	• Liste des types de données traités • Présence d'informations sensibles dans les données traitées (par ex. concernant la santé)
Stockage des données RFID	• Liste des types de données stockés • Durée du stockage
Transfert interne de données RFID (le cas échéant)	• Description ou diagrammes portant sur les flux de données dans le cadre des opérations internes concernant des données RFID • Objectif(s) d'un transfert des données à caractère personnel
Transfert externe de données RFID (le cas échéant)	• Type de destinataire(s) des données • Objectif(s) du transfert ou de l'accès en général • Données à caractère personnel identifiées et/ou identifiables concernées par le transfert (ou niveau de ces données) • Transferts en dehors de l'Espace économique européen (EEE)

ANNEXE II – *Objectifs en matière de respect de la vie privée*

La directive 95/46/CE énonce actuellement neuf objectifs en matière de respect de la vie privée. Le processus d'EIVP a été élaboré en prenant en considération ces objectifs et les risques associés inhérents aux RFID. La présente annexe résume ces objectifs. Si tous sont des éléments essentiels de la conformité sur le plan de l'organisation, seule une partie des exigences qu'ils impliquent sera généralement pertinente pour l'application RFID examinée. Ces objectifs ont donc pour rôle d'inspirer la création et le développement du processus d'EIVP plus que la réalisation d'une EIVP particulière.

Description des objectifs en matière de respect de la vie privée (extraits actualisés de la/des directive(s) européenne(s) en la matière; en l'occurrence la directive 95/46/CE)	
Préservation de la qualité des données à caractère personnel	Éviter et limiter au maximum les données, spécifier et limiter la finalité de la collecte, assurer la qualité des données et la transparence sont les principaux objectifs à atteindre.
Légitimité du traitement des données à caractère personnel	La légitimité du traitement des données à caractère personnel doit être assurée en fondant ce dernier sur le consentement, la relation contractuelle, l'obligation légale, etc.
Légitimité du traitement des données à caractère personnel sensibles	La légitimité du traitement des données à caractère personnel sensibles doit être assurée en fondant ce dernier sur le consentement explicite, une base juridique spécifique, etc.
Respect du droit à l'information de la personne concernée	Il convient de veiller à ce que la personne concernée soit informée en temps opportun de la collecte de ses données.
Respect du droit de la personne concernée d'accéder à ses données, de les corriger et de les effacer.	Il convient de s'assurer que la personne concernée qui le souhaite puisse, en temps opportun, accéder à ses données et les corriger, les effacer et les verrouiller.
Respect du droit d'opposition de la personne concernée	Il convient de mettre un terme au traitement des données de la personne concernée lorsque celle-ci s'oppose à ce traitement. La transparence des décisions automatisées vis-à-vis des personnes doit particulièrement être assurée.
Préservation de la confidentialité et de la sécurité du traitement	Prévenir l'accès non autorisé aux données, consigner le traitement des données, assurer la sécurité du réseau et du transport et prévenir toute perte accidentelle de données sont les principaux objectifs à atteindre.
Respect des obligations de notification	La notification relative au traitement des données, le contrôle préalable de la conformité et la consignation sont les principaux objectifs à atteindre.
Respect des obligations en matière de conservation des données	Les données doivent être conservées le moins longtemps possible, compte tenu de la finalité de la conservation ou de toute autre disposition juridique.

ANNEXE III – *Risques en matière de respect de la vie privée*

La présente section contient une liste de risques potentiels pour la vie privée liés à l'utilisation de l'application RFID examinée. Il est recommandé, notamment pour les EIVP complètes, d'identifier systématiquement les risques au moyen de procédures standard d'évaluation des risques couvrant les risques liés à une application RFID et les vulnérabilités face à une telle application.

Le tableau ci-dessous fournit des exemples de risques susceptibles d'affecter la capacité d'une entité d'atteindre les objectifs en matière de respect de la vie privée décrits à l'annexe II. Les exploitants d'applications RFID peuvent utiliser cette liste comme point de départ. Ces risques ne s'appliquent cependant pas forcément tous à toutes les applications RFID. Les exploitants d'applications RFID doivent s'assurer que chacun des risques décelés soit correctement limité par un ou plusieurs dispositifs de contrôle en fonction de la probabilité que ce risque ne se matérialise et de l'ampleur de l'impact. Ils pourraient être amenés à combiner différents dispositifs de contrôle ou à renforcer les dispositifs existants, en fonction de facteurs tels que les technologies utilisées, la nature de leur mise en œuvre, le type d'informations et les politiques applicables.

Risque en matière de respect de la vie privée	**Description et exemple**
Finalité non spécifiée et non limitée	La finalité de la collecte des données n'a pas été spécifiée et consignée, ou les données utilisées sont plus nombreuses que nécessaire pour la finalité spécifiée. Exemple: la finalité de l'utilisation des données RFID n'est pas consignée et/ou les données RFID sont utilisées pour toutes sortes d'analyses potentielles.
Collecte supérieure à la finalité	Les données sont collectées sous une forme identifiable allant au-delà de la finalité spécifiée. Exemple: les informations d'une carte de paiement RFID ne sont pas utilisées aux seules fins du traitement des transactions, mais aussi pour établir des profils individuels.
Informations incomplètes ou manque de transparence	Les informations fournies à la personne concernée concernant la finalité et l'utilisation des données sont incomplètes, le traitement des données manque de transparence ou les informations ne sont pas communiquées en temps opportun. Exemple: les informations RFID communiquées aux consommateurs ne précisent pas assez clairement la manière dont les données RFID sont traitées et exploitées, l'identité de l'exploitant ou les droits de l'utilisateur.

Interconnexion supérieure à la finalité	Les données à caractère personnel sont interconnectées au-delà de ce qui est nécessaire pour atteindre l'objectif spécifié. Exemple: les informations d'une carte de paiement RFID sont interconnectées avec les données à caractère personnel provenant d'une tierce partie.
Absence de politiques ou de mécanismes d'effacement	Les données sont conservées plus longtemps que nécessaire pour atteindre l'objectif spécifié. Exemple: des données à caractère personnel sont collectées dans le cadre de l'application et sont sauvegardées pour une période plus longue que ce qu'autorise la loi.
Invalidation du consentement explicite	Le consentement a été obtenu sous la menace de conditions défavorables. Exemple: impossibilité de retourner/d'échanger un produit ou de bénéficier des garanties légales le concernant lorsque l'étiquette RFID est désactivée ou enlevée.
Collecte secrète de données par l'exploitant d'application RFID	Certaines données sont enregistrées en secret, et donc sans que la personne concernée en soit informée – ex.: profil de déplacement. Exemple: des informations concernant le client sont lues lorsque ce dernier passe devant un magasin ou se déplace dans un centre commercial, alors qu'aucun logo et aucun signe ne l'informe de la lecture de données RFID.
Impossibilité pour la personne concernée d'accéder à ses données	La personne concernée n'a aucun moyen de faire corriger ou effacer ses données. Exemple: un employeur ne peut indiquer exactement à son employé quelles sont les informations enregistrées le concernant à partir d'un accès RFID et des données de fabrication.
Impossibilité de s'opposer	Il n'existe aucun moyen technique ou opérationnel de répondre à l'opposition d'une personne concernée. Exemple: dans un hôpital, un visiteur ne peut s'opposer à la lecture d'informations à caractère personnel sensibles à partir d'étiquettes (par exemple concernant des traitements).
Manque de transparence des décisions individuelles automatisées	Des décisions individuelles automatisées reposant sur des éléments personnels sont utilisées, mais les personnes concernées ne sont pas informées de la logique sous-tendant la prise de décisions. Exemple: sans en informer ses clients, un exploitant d'application RFID procède à la lecture de toutes les étiquettes portées par une

	personne, dont celles provenant d'une autre entité, et détermine le type de messages promotionnels à envoyer à cette personne en fonction de ces étiquettes.
Manquements dans la gestion des droits d'accès	Les droits d'accès ne sont pas retirés lorsqu'ils ne se justifient plus. Exemple: grâce à une carte RFID, un ancien stagiaire peut accéder à certaines parties d'une entreprise alors qu'il ne devrait pas y être autorisé.
Manquements au niveau du mécanisme d'authentification	Rien n'est fait pour empêcher un nombre suspect de tentatives d'identification et d'authentification. Exemple: les données à caractère personnel contenues dans les étiquettes ne sont pas protégées par défaut par un mot de passe ou par un autre mécanisme d'authentification.
Traitement de données illégitime	Le traitement des données à caractère personnel ne repose pas sur le consentement, sur une relation contractuelle, sur une obligation légale, etc. Exemple: un exploitant d'application RFID partage les informations qu'il a collectées avec une tierce partie sans en informer les personnes concernées ou sans l'accord de ces dernières, contrairement à la législation.
Manquements au niveau du mécanisme de consignation	Le mécanisme de consignation mis en œuvre présente des insuffisances. Il ne consigne pas les processus administratifs. Exemple: le nom des personnes qui ont consulté les données d'une carte d'employé RFID n'est pas consigné.
Impossibilité de contrôler l'acquisition de données provenant d'étiquettes RFID	Le risque existe que les étiquettes RFID soient utilisées pour établir le profil de personnes et/ou les suivre à la trace. Exemple: un détaillant lit toutes les étiquettes qu'il est en mesure de lire.

ANNEXE IV – *Exemples de dispositifs de contrôle des applications RFID et de mesures de limitation des risques*

La présente section contient une liste d'exemples de dispositifs de contrôle potentiels susceptibles d'aider un exploitant d'application RFID à déterminer les stratégies adaptées de limitation des risques. Les risques définis comme pertinents pour un exploitant d'application RFID durant l'étape n° 2 de la phase d'évaluation des risques du processus d'EIVP peuvent être limités au moyen d'une ou de plusieurs stratégies de limitation des risques, dont certaines sont présentées dans la présente annexe. L'objectif poursuivi est qu'en réalisant une EIVP, l'exploitant d'application RFID identifie et entreprenne les contrôles nécessaires pour limiter les risques pertinents en matière de vie privée.

Les mécanismes de contrôle potentiels sont notamment:

- les pratiques de gestion de l'application RFID;
- l'accès individuel et le contrôle;
- les mesures de protection du système (y compris les contrôles de sécurité);
- la protection des étiquettes;
- les mesures en matière de responsabilité.

Ces pratiques sont subordonnées au cadre réglementaire actuel de l'Union européenne en matière de protection des données et ne sont aucunement destinées à le remplacer ou à en modifier le champ d'application.

Pratiques de gestion de l'application RFID

Les pratiques de gestion peuvent inclure:

- les pratiques de gestion mises en œuvre par l'exploitant d'application RFID;
- les politiques de suppression et d'effacement des données RFID;
- les politiques relatives à un traitement légal des informations à caractère personnel;
- les dispositions en faveur d'une limitation maximale des données lors du traitement des données RFID lorsque la situation le permet;
- le traitement ou le stockage des informations provenant d'étiquettes qui n'appartiennent pas à l'exploitant d'application RFID;
- les pratiques de gestion de la sécurité.

Fourniture d'accès individuel et contrôle

- Fourniture d'informations relatives aux finalités du traitement et aux catégories de données à caractère personnel concernées.

- Description de la manière de s'opposer au traitement des données à caractère personnel ou de retirer son consentement.

- Détermination du processus de demande de rectification ou d'effacement de données à caractère personnel incomplètes ou inexactes.

Protection du système

La **protection du système** sous l'angle de la protection adaptée de la vie privée et des données à caractère personnel doit également être décrite dans cette section du rapport d'EIVP. Les concepts de protection du système s'appliquent aux systèmes dorsaux et aux infrastructures de communication dans la mesure où ils concernent l'application RFID. Lorsqu'ils s'appliquent, il convient de reconnaître que les systèmes dorsaux sont souvent complexes et qu'ils peuvent avoir fait l'objet d'une EIVP spécifique. Il est possible que cette analyse doive être réexaminée pour s'assurer qu'elle a pris en considération les informations de la nature de celles utilisées par l'application RFID. En l'absence d'une telle EIVP, les éléments suivants du système dorsal doivent être contrôlés:

- la présence de dispositifs de contrôle de l'accès adaptés au type de données à caractère personnel et à la fonctionnalité des systèmes;

- les contrôles et les politiques mis en place pour garantir que l'exploitant ne relie pas les données à caractère personnel de l'application RFID d'une manière non conforme au rapport d'EIVP;

- la présence ou l'absence de mesures appropriées afin de préserver la confidentialité, l'intégrité et la disponibilité des données à caractère personnel au niveau des systèmes et de l'infrastructure de communication;

- les politiques relatives à la conservation et à la suppression des données à caractère personnel;

- l'existence et la mise en œuvre de contrôles portant sur la sécurité de l'information, tels que:

    - des mesures portant sur la sécurité des réseaux et le transport des données RFID;

    - des mesures améliorant la disponibilité des données RFID grâce à des sauvegardes et à une récupération appropriées.

Protection des étiquettes RFID

Les dispositifs de contrôle assurant la **protection des étiquettes RFID** sur le plan de la vie privée et des données à caractère personnel devraient être mentionnés. Ils revêtent une importance toute particulière pour les applications RFID qui utilisent des étiquettes RFID contenant des données à caractère personnel.

Ces dispositifs de protection comprennent les éléments suivants:

- contrôle de l'accès aux fonctionnalités et aux informations, comprenant l'authentification des lecteurs, des scripteurs et des processus sous-jacents ainsi que l'autorisation d'agir sur l'étiquette RFID;

- méthodes destinées à garantir/gérer la confidentialité de l'information (par exemple par le cryptage de l'ensemble de l'étiquette RFID ou de certains champs);

- méthodes destinées à garantir/gérer l'intégrité de l'information;

- conservation des informations après la collecte initiale (par exemple durée de conservation, procédures d'élimination des données au terme de la période de conservation ou d'effacement des informations contenues dans l'étiquette RFID, procédures de conservation ou de suppression de certains champs);

- inviolabilité de l'étiquette RFID elle-même;

- désactivation ou retrait, en cas de besoin ou d'instructions en ce sens.

Les mesures de limitation des risques peuvent comprendre des contrôles axés sur les utilisateurs lors desquels sont traitées des situations pouvant impliquer différents besoins ou différentes sensibilités en matière de vie privée. La désactivation et le retrait sont actuellement les deux formes les plus courantes de limitation des risques axées sur le consommateur ou l'utilisateur final. Ils peuvent s'imposer à l'issue d'une analyse d'EIVP, en vertu de la loi dans certaines circonstances, ou en tant qu'option proposée au consommateur après la vente pour renforcer la confiance dudit consommateur. La recommandation européenne sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications RFID propose en outre certaines méthodes et bonnes pratiques concernant le processus de désactivation ou de retrait dans le commerce de détail[4].

Mesures en matière de responsabilité

Ces mesures portent sur la protection procédurale des données du point de vue de la responsabilité. Elles permettent une prise de conscience à l'extérieur concernant les applications RFID.

- Mettre en place une **politique de l'information** axée sur un accès facile à des informations exhaustives comprenant:

    - l'identité et l'adresse de l'exploitant d'application RFID;

    - la finalité de l'application RFID;

    - les types de données traités par l'application RFID, notamment en cas de traitement de données à caractère personnel;

    - le contrôle ou pas de la localisation des étiquettes RFID lorsqu'elles seront en la possession d'une personne;

    - le cas échéant, les incidences probables, sur le plan du respect de la vie privée et de la protection des données, de l'utilisation des étiquettes RFID contenues dans l'application RFID, ainsi que les mesures adoptées pour limiter ces impacts.

[4] Points 12 et 13 de la recommandation CE du 12 mai 2009. {SEC (2009) 585}: Toute méthode de désactivation ou de retrait doit être proposée gratuitement, dans l'immédiat ou ultérieurement, sans réduction ou cessation des obligations légales du détaillant ou du fabricant envers le consommateur.

- **Signaler** de manière concise, claire et précise la présence de lecteurs RFID, en mentionnant:
    - l'identité de l'exploitant d'application RFID;
    - un point de contact où obtenir des renseignements sur la politique d'information.
- Indiquer s'il existe des **voies de recours** et, le cas échéant, comment les actionner:
    - entité(s) juridique(s) responsable(s) de l'exploitant d'application RFID (éventuellement une par juridiction ou zone d'exploitation);
    - point(s) de contact de la personne ou du bureau chargé(e) de réexaminer les évaluations et l'adéquation constante des mesures techniques et organisationnelles relatives à la protection des données à caractère personnel et au respect de la vie privée;
    - canaux de renseignement (par exemple, moyens de contacter l'exploitant de l'application RFID pour lui poser une question, introduire une demande, déposer une plainte ou exercer un droit);
    - marche à suivre pour s'opposer au traitement de données, exercer ses droits d'accès aux données à caractère personnel (y compris suppression et correction de ces données) ou retirer son accord, ou pour modifier les dispositifs de contrôle et opérer d'autres choix concernant le traitement de données à caractère personnel, en cas de besoin ou d'instructions en ce sens;
    - autres voies de recours, en cas de besoin ou d'instructions en ce sens.

Annexe A: références

La présente section contient les références des documents officiels utilisés pour l'élaboration du cadre.

- «Recommandation de la Commission sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence», Commission des communautés européennes, 12 mai 2009, C (2009) 3200, disponible à l'adresse: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:FR:PDF.

- «Commission staff working document accompanying the Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio frequency identification», résumé de l'évaluation d'impact, Commission des communautés européennes, 12 mai 2009, SEC(2009) 586, disponible (en anglais) à l'adresse: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf.

- «Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données», Journal officiel des Communautés européennes, 23 novembre 1995, L 281/31, disponible à l'adresse: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:FR:PDF.

- «Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)», Journal officiel des Communautés européennes, 31 juillet 2002, L 201/37, disponible à l'adresse: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:FR:PDF.

- «Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs», Journal officiel de l'Union européenne, 18 décembre 2009, L 337/11, disponible à l'adresse: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:FR:PDF.

- «Avis 4/2007 sur le concept de données à caractère personnel», groupe de travail «article 29» sur la protection des données, 20 juin 2007, 01248/07/FR WP 136, disponible à l'adresse: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf.

- «Privacy Impact Assessment Handbook», disponible (en anglais) à l'adresse: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

- «Status of Implementation of Directive 95/46 on the protection of Individuals in regards to the Processing of Personal Data», disponible (en anglais) à l'adresse: http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.

- «Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)», groupe de travail «article 29» sur la protection des données, 19 janvier 2005, 10107/05/FR WP 105, disponible à l'adresse: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_fr.pdf.

Annexe B: glossaire

Plusieurs termes et expressions utilisés dans le présent cadre sont associés au concept de respect de la vie privée et de protection des données et à l'utilisation de la technologie RFID dans toute une série de contextes. Aux fins du présent cadre, les définitions données dans la directive 95/46/CE sont d'application concernant le respect de la vie privée et la protection des données.

Les définitions ci-dessous concernent la technologie RFID et ses applications et s'appliquent au présent cadre.

Personne: toute personne physique qui interagit avec un ou plusieurs composants d'une application RFID (par exemple système dorsal, infrastructure de communication, étiquette RFID) ou qui leur est associée d'une autre manière sans exploiter elle-même une application RFID ou exercer l'une de ses fonctions. En ce sens, une personne diffère d'un utilisateur. Une personne peut ne pas être directement associée au fonctionnement de l'application RFID mais, par exemple, simplement détenir un objet équipé d'une étiquette RFID.

Sécurité de l'information: préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information.

Suivi: toute activité exercée afin de détecter, d'observer, de copier ou d'enregistrer la localisation, les déplacements, les activités ou l'état d'une personne.

Données à caractère personnel: toute information concernant une personne physique identifiée ou identifiable («personne concernée»); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Application RFID: une application qui traite des données par l'utilisation d'étiquettes et de lecteurs et qui repose sur un système dorsal et une infrastructure de communication en réseau.

Exploitant d'application RFID: la personne physique ou morale, l'organisme public, l'agence ou tout autre organe qui, seul ou avec d'autres, définit la finalité et les modalités de l'exploitation d'une application, y compris les responsables du traitement des données à caractère personnel utilisant une application RFID.

Identification par radiofréquence (RFID): l'utilisation d'ondes électromagnétiques rayonnantes ou d'un couplage de champ réactif dans une portion de radiofréquences du spectre pour communiquer vers ou à partir d'une étiquette selon différents schémas de modulation et d'encodage afin de lire, de façon univoque, l'identité d'une étiquette de radiofréquence ou d'autres données stockées sur celle-ci.

Lecteur RFID: un dispositif fixe ou mobile d'identification et de saisie de données utilisant une onde électromagnétique de radiofréquence ou un couplage de champ réactif pour stimuler et effectuer une réponse de donnée modulée à partir d'une étiquette ou d'un groupe d'étiquettes.

Étiquette RFID ou «étiquette»: un dispositif RFID ayant la capacité de produire un signal radio ou un dispositif RFID qui raccorde, rétrodiffuse ou reflète (selon le type de dispositif) et module un signal porteur reçu d'un lecteur ou scripteur.

Information de l'étiquette RFID ou information contenue dans l'étiquette RFID: l'information contenue dans une étiquette RFID et transmise lorsque cette dernière est sollicitée par un lecteur RFID.

Utilisateur: spécifiquement, un utilisateur d'application RFID, c'est-à-dire une personne (ou une autre entité, par exemple une entité juridique) qui interagit directement avec un ou plusieurs composants d'une application RFID (par exemple système dorsal, infrastructure de communication, étiquette RFID) afin d'exploiter une application RFID ou d'exercer une ou plusieurs de ses fonctions.