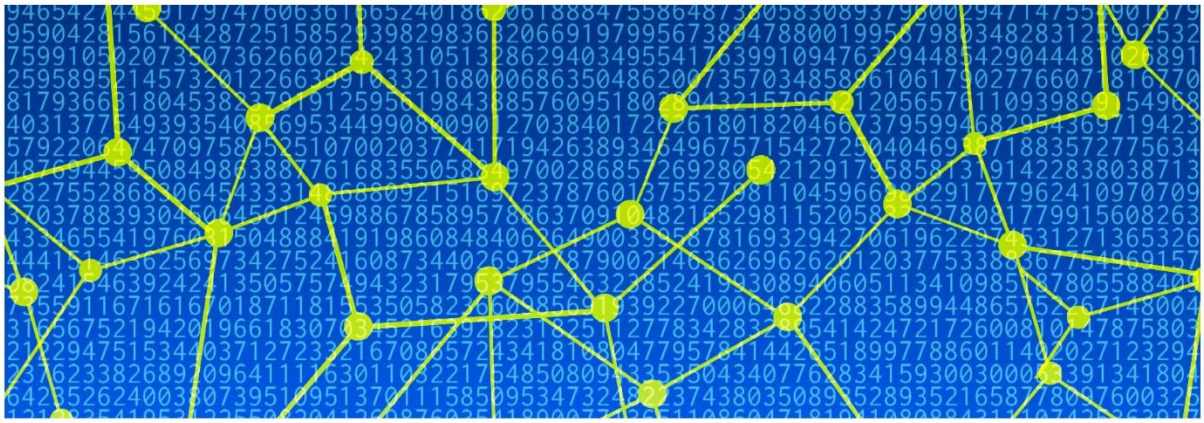

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 9/2016

Avis du CEPD sur les systèmes de gestion des informations personnelles

Vers une plus grande autonomie des utilisateurs dans la gestion et le traitement des données à caractère personnel

EDPS

20 octobre 2016

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne chargée, en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires» et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, «lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel», la Commission a l'obligation de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis se rapporte à la mission du CEPD de conseil des institutions de l'Union sur les implications de leurs politiques en matière de protection des données et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Le CEPD considère que l'environnement émergent des systèmes de gestion des informations personnelles (Personal Information Management Systems, PIMS), qui visent à permettre aux personnes physiques et aux consommateurs de reprendre le contrôle de leurs données à caractère personnel, mérite d'être pris en considération afin de contribuer à une utilisation durable et éthique des données massives et à la mise en œuvre effective des principes du règlement général sur la protection des données (RGPD), récemment adopté.

Synthèse

Le présent avis étudie le concept de technologies et d'écosystèmes visant à habiliter les personnes à contrôler le partage de leurs données à caractère personnel («systèmes de gestion des informations personnelles», ou «PIMS» en abrégé).

Notre vision est de créer une réalité nouvelle où les personnes gèrent et contrôlent leur identité en ligne. Notre but est de transformer le système actuel, centré sur les fournisseurs, en un système centré sur l'humain, qui protège les personnes du traitement illicite de leurs données et des techniques intrusives de traçage et de profilage tendant à contourner les principes fondamentaux de la protection des données.

Cette réalité nouvelle sera facilitée par le cadre réglementaire actualisé de l'Union européenne et par les possibilités découlant d'une application rigoureuse et conjointe de la législation par l'ensemble des autorités compétentes en matière de contrôle et de réglementation.

Le règlement général sur la protection des données récemment adopté renforce et modernise le cadre réglementaire de manière à ce qu'il reste efficace à l'ère des données massives en raffermissant la confiance des personnes dans la sécurité en ligne et le marché unique numérique. Les nouvelles règles, notamment celles concernant la transparence accrue et les puissants droits d'accès et de portabilité des données, visent à permettre aux utilisateurs de mieux contrôler leurs données. Elles peuvent également contribuer à l'efficacité des marchés de données à caractère personnel, dans l'intérêt des consommateurs et des entreprises.

Récemment encore, nous avons rendu un avis sur l'application effective des droits fondamentaux à l'ère des données massives. Celui-ci met en évidence les conditions du marché et les pratiques des entreprises qui font obstacle à l'exercice effectif des droits des personnes à la protection de leurs données à caractère personnel ainsi que d'autres droits fondamentaux. Il demande de redoubler d'efforts pour faire appliquer de manière concertée et cohérente la législation en matière de concurrence et de protection des consommateurs et des données. Nous espérons que cette meilleure application de la législation contribuera à créer des conditions du marché dans lesquelles les services qui respectent la vie privée pourront prospérer. L'approche développée dans le présent avis vise à renforcer les droits fondamentaux dans cet univers numérique qui est le nôtre, tout en envisageant des possibilités nouvelles qui permettront aux entreprises de développer des services innovants basés sur les données à caractère personnel et reposant sur une confiance mutuelle. Les PIMS promettent non seulement une nouvelle architecture technique et une nouvelle organisation de la gestion des données, mais aussi des cadres basés sur la confiance et, de ce fait, des modèles commerciaux différents pour collecter et traiter les données à caractère personnel à l'ère des données massives d'une manière plus respectueuse de la législation européenne en matière de protection des données.

Dans le présent avis, nous expliquerons brièvement en quoi les PIMS consistent, les problèmes qu'ils sont censés résoudre et les solutions qu'ils mettent en œuvre à cet effet. Nous analyserons ensuite la contribution qu'ils peuvent apporter à l'amélioration de la protection des données à caractère personnel, ainsi que les défis qui les attendent. Enfin, nous dégagerons des pistes permettant d'exploiter les possibilités qu'ils offrent. Pour que les nouveaux modèles commerciaux dans le domaine de la protection des données prospèrent, il sera peut-être nécessaire d'adopter des mesures d'incitation supplémentaires à l'intention des fournisseurs de services qui les offrent. Il convient d'examiner en particulier les initiatives politiques susceptibles d'encourager les responsables du traitement des données à accepter cette nouvelle manière de fournir des données. En outre, une initiative des services publics visant à accepter

les PIMS comme source de données en remplacement de la collecte directe de données pourrait favoriser l'acceptation des PIMS.

L'environnement émergent des PIMS, qui visent à permettre aux personnes et aux consommateurs de reprendre le contrôle de leurs données à caractère personnel, mérite d'être pris en considération, soutenu et mieux étudié afin de contribuer à une utilisation durable et éthique des données massives et à la mise en œuvre effective des principes du RGPD récemment adopté.

TABLE DES MATIÈRES

1. PIMS: UN PARTAGE DE DONNÉES MUTUELLEMENT PROFITABLE?

1 Les conditions actuelles du traitement de données à caractère personnel sont souvent inéquitables pour les personnes dont les données sont traitées. Les conditions juridiques et les outils techniques empêchent les personnes d'exercer aisément leurs droits et permettent aux responsables du traitement de limiter leur responsabilité. Les courtiers en données, les réseaux publicitaires, les fournisseurs de réseaux sociaux et d'autres acteurs économiques détiennent des fichiers de plus en plus complets sur les personnes participant à la société numérique actuelle, qui perdent le contrôle des empreintes numériques qu'elles laissent derrière elles. Ciblées, profilées et évaluées par des acteurs hors de leur portée ou dont elles ne soupçonnent même pas l'existence, les personnes peuvent se sentir démunies. Elles doivent être habilitées à prendre le contrôle de leur identité. Même lorsqu'elles ont officiellement reçu une forme ou l'autre de «notification» et qu'elles ont eu l'occasion de «consentir» aux conditions générales, les personnes se retrouvent souvent dans un système conçu pour maximiser la monétisation des données à caractère personnel, sans leur laisser vraiment ni le choix ni une possibilité de contrôle.

2 La communication de la Commission européenne relative aux données massives[1] expose un plan d'actions axées à la fois sur les données à caractère personnel et sur la protection des consommateurs. Elle encourage en particulier l'utilisation d'«espaces de données personnelles» en tant qu'espaces sûrs et sécurisés, centrés sur l'utilisateur, pour stocker des données à caractère personnel et éventuellement permettre à des tiers d'y accéder. Nous sommes d'avis qu'il convient d'encourager les outils numériques et les modèles commerciaux innovants basés sur l'autonomisation des personnes. Les personnes pourraient ainsi bénéficier d'un tel partage de données, c'est-à-dire participer à l'utilisation et à la diffusion de leurs informations personnelles.

3 Dans notre avis intitulé «Relever les défis des données massives»[2], nous avons fait valoir que l'obligation légale concernant le consentement effectif devrait être complétée par un contrôle réel et pratique sur les informations personnelles. Nous avons expliqué que «*plutôt qu'une charge administrative, la fourniture de droits d'accès pourrait devenir une caractéristique du service offert aux clients*» et que les organisations qui exploitent les «données massives» «*devraient être prêtes à partager les profits générés par le traitement des données à caractère personnel avec les personnes concernées dont les données sont traitées*». Dans ce contexte, nous avons noté que les «*entrepôts de données personnelles pourraient aider à dissiper certaines des inquiétudes concernant la perte du contrôle individuel sur les données à caractère personnel*». Le règlement général sur la protection des données (RGPD) récemment adopté[3] a renforcé les exigences légales de consentement[4] et introduit les principes modernes et efficaces de protection dès la conception et par défaut[5], ainsi qu'un droit nouveau à la portabilité des données[6]. Pour que le nouveau cadre relatif à la protection des données remplisse ses promesses, nous avons besoin d'outils pratiques qui permettront aux personnes d'exercer leurs droits d'une manière pratique et conviviale.

4 Le présent avis étudie les nouvelles technologies et les écosystèmes visant à habiliter les personnes à contrôler la collecte et le partage de leurs données à caractère personnel. Nous désignerons ce concept sous le vocable de «système de gestion des informations personnelles» («PIMS»)[7]. Le concept de PIMS offre une nouvelle approche qui consiste à faire des personnes les détenteurs de leurs propres informations personnelles. Il pourrait entraîner un changement de paradigme dans la gestion et le traitement des données à

caractère personnel et avoir des conséquences sur le plan social et économique. Par comparaison, l'environnement actuel des services en ligne se caractérise par un nombre restreint de fournisseurs de services qui dominent le marché en monétisant les données à caractère personnel des utilisateurs en échange de services «gratuits». Cela va souvent de pair avec une relation déséquilibrée, dans laquelle le client se voit proposer une offre «à prendre ou à laisser», et avec une information asymétrique entre les fournisseurs de services et les utilisateurs caractérisée par une transparence limitée, voire inexistante, sur le sort réservé aux données à caractère personnel des personnes.

5 L'idée maîtresse qui sous-tend le concept de PIMS est de transformer le système actuel, centré sur les fournisseurs, en un système centré sur des personnes capables de gérer et de contrôler leur identité en ligne[8]. En principe, les personnes devraient être en mesure de décider si elles partagent leurs informations personnelles et avec qui, pour quelles finalités et pour quelle durée, ainsi que de conserver la trace de ces données et de décider de les retirer si elles le souhaitent. Il serait utile d'étudier de quelle manière les PIMS pourraient aider à dissiper certaines des inquiétudes concernant la perte du contrôle individuel sur les données à caractère personnel, qui ressort comme étant l'une des principales préoccupations soulevées par les données massives[9].

6 Cette approche vise à renforcer les droits fondamentaux dans cet univers numérique qui est le nôtre, tout en envisageant des possibilités nouvelles qui permettront aux entreprises de développer des services innovants basés sur les données à caractère personnel et reposant sur une confiance mutuelle. Les PIMS promettent une nouvelle architecture technique et une nouvelle organisation de la gestion des données qui mettent en place des cadres basés sur la confiance. Ils cherchent à rendre possibles des modèles commerciaux différents de collecte et de traitement des données à caractère personnel à l'ère des données massives d'une manière plus respectueuse de la législation européenne en matière de protection des données.

7 Dans le présent avis, nous expliquerons brièvement en quoi les PIMS consistent, les problèmes qu'ils sont censés résoudre et les solutions qu'ils mettent en œuvre à cet effet[10]. Nous analyserons la contribution qu'ils peuvent apporter à l'amélioration de la protection des données à caractère personnel, ainsi que les défis qui les attendent. Enfin, nous dégagerons des pistes permettant d'exploiter les possibilités qu'ils offrent.

2. MODÈLES ET CARACTÉRISTIQUES DES PIMS ÉMERGENTS

2.1. Architecture et technologie

8 Les PIMS en sont à un stade précoce de leur développement. La manière dont ils sont conçus et les modèles commerciaux qui les sous-tendent sont très différents. L'expérience relative à leur utilisation pratique et à leur incidence sur le traitement des informations personnelles est limitée. La présente section expose certains modèles et caractéristiques des PIMS émergents.

Où sont les données?

9 Une distinction importante peut être opérée entre les divers types de PIMS émergents en fonction de leur architecture technique, selon qu'elle repose sur un entreposage local ou sur un entreposage en nuage. Dans le modèle basé sur l'entreposage local, les données à caractère personnel sont conservées dans les appareils des usagers tels que les ordinateurs

portables, les téléphones intelligents, les tablettes, etc. Dans le modèle en nuage, les données des utilisateurs sont essentiellement conservées par des fournisseurs de services (réseaux sociaux, suites bureautiques en ligne, prestataires de soins de santé, etc.) ainsi que par des fournisseurs spécialisés de PIMS en nuage.

10 Dans la configuration en nuage, deux types d'approches fondamentales peuvent également exister l'une à côté de l'autre. Certains PIMS sont conçus pour conserver les données des utilisateurs à un endroit unique; d'autres créent un lien logique entre ces données, qui peuvent rester chez divers fournisseurs de services.

Comment les données sont-elles traitées?

11 Soit les données ne quittent pas le PIMS (et dans certains modèles, des algorithmes sont même importés et calculés en interne), soit elles sont transférées en toute sécurité aux fournisseurs de services, qui peuvent également les stocker sous une forme chiffrée en vue des opérations de traitement. Les données et leurs propriétés sont conservées dans un format interopérable et lisible par machine, qui permet des interactions sans intervention humaine.

Comment la sécurité et la protection des données sont-elles mises en œuvre?

12 La sécurité et la protection des données sont les principales raisons d'être des PIMS. La cryptographie joue un rôle fondamental et constitue un élément nécessaire de la sécurité des données et de la confiance mutuelle que toutes les parties prenantes à la chaîne de traitement des données vouent à l'authenticité et à l'intégrité des données:

a) le chiffrement peut garantir la confidentialité des données statiques ou en transit;

b) des fonctions cryptographiques pourraient être utilisées pour vérifier l'authenticité des données et appliquer les préférences des utilisateurs en matière de vie privée, par exemple, les finalités et les durées de conservation autorisées à l'égard des fournisseurs de services et des tiers.

13 Dans certains modèles, des tiers (entités publiques ou privées) jouent le rôle de nouveaux acteurs des écosystèmes de gestion de données en fournissant des services de confiance. Leur rôle est de susciter la confiance réciproque, principalement entre les utilisateurs et les fournisseurs de services, en fournissant des identités, dont ils sont aussi les gardiens, en facilitant les mécanismes d'autorisation et en permettant la traçabilité des données à caractère personnel et des opérations de traitement qu'elles subissent.

14 Des services de minimisation des données et d'anonymisation sont également fournis. Par exemple, il peut être possible d'effectuer une transaction lorsque l'autorisation n'est pas conditionnée à une divulgation de l'identité complète (par exemple, le PIMS peut confirmer qu'un utilisateur remplit la condition liée à l'âge, au lieu de demander son nom et sa date de naissance)[11]. Dans d'autres cas, les PIMS offrent des services d'anonymat[12] vis-à-vis des fournisseurs de services et des autres parties qui utilisent les données, par exemple, en agrégeant celles-ci avant de les leur transférer[13].

2.2. Principales caractéristiques facilitant le contrôle des personnes sur leurs données à caractère personnel

15 L'un des principaux objectifs des PIMS est de permettre aux utilisateurs de définir avec suffisamment de précision comment leurs informations personnelles doivent être utilisées et à quelles fins et de conserver la trace de la façon dont ces informations sont utilisées afin d'avoir la certitude qu'elles ne sont pas traitées d'une manière non autorisée. Cela implique

une fonction étendue de gestion du consentement qui permet aussi aux utilisateurs de retirer leur consentement lorsqu'ils le souhaitent. Habituellement, un tableau de bord convivial est prévu à cet effet. Les autres parties (les autres utilisateurs et les fournisseurs de services) sont généralement en mesure d'accéder automatiquement aux données en fonction des préférences retenues pour protéger la vie privée.

16 Outre la gestion des identifications, des autorisations et des préférences en matière de vie privée, les PIMS fournissent souvent d'autres services à valeur ajoutée. Certains PIMS offrent la possibilité d'extraire des données sur la présence en ligne de l'utilisateur (comme l'historique de navigation, les signets, les carnets d'adresses, les justificatifs d'identité, les données de localisation, les données financières ou les activités sur les réseaux sociaux). Ces données sont alors organisées au sein des PIMS.

17 Une évolution intéressante des PIMS est la possibilité d'inclure des caractéristiques d'analyse personnelle. Cela soutiendrait le nouveau paradigme dans lequel les utilisateurs contrôlent leurs données et ce que ces données révèlent à leur sujet. Dans un monde hypothétique où l'utilisateur a accès à toutes les informations qui le concernent, celui-ci pourrait disposer d'un assistant personnel qui contrôlerait, dans le respect de sa vie privée, la manière dont les informations tirées de son fichier personnel de données massives sont utilisées. Cela pourrait se faire dans un contexte propre à un secteur (par exemple, pour les données liées au bien-être et à la santé ou la mobilité personnelle) ou dans une perspective globale, par agrégation des données relatives à une personne recueillies à partir de différentes sources et dans divers contextes. Les utilisateurs contrôleraient la manière dont leurs informations personnelles et/ou les connaissances qui en sont déduites sont partagées avec des tiers, dans le respect de leurs préférences et d'une manière qui soit profitable à chacune des parties.

2.3. Cadre politique et modèles commerciaux relatifs aux PIMS

18 Les PIMS nécessitent plus qu'une nouvelle architecture de gestion des données basée sur une technologie adéquate. Une politique adoptée d'un commun accord, la confiance dans sa mise en œuvre et des mécanismes permettant de contrôler et de vérifier cette confiance et de remédier aux problèmes sont également essentiels pour garantir une sécurité et une protection efficaces des données dans un environnement autorégulé en s'appuyant sur le cadre juridique.

19 Certaines organisations[14] proposent, par conséquent, des PIMS dans lesquels la sûreté de la gestion des données à caractère personnel et le respect de la vie privée sont assurés par la contribution de nombreux acteurs jouant des rôles différents, dans le respect d'une politique ad hoc et d'un système de gouvernance. L'idée est de créer de nouvelles communautés de confiance basées sur la transparence et l'équité, où les fournisseurs de services en ligne traditionnels, les nouveaux acteurs économiques (par exemple, les fournisseurs de services de PIMS et les fournisseurs de services de confiance) et les personnes dont les données à caractère personnel sont gérées et traitées peuvent bénéficier chacun d'une part équitable des avantages des données massives.

20 Les modèles commerciaux qui prédominent actuellement parmi les fournisseurs de PIMS (et les autres acteurs qui rendent possible l'écosystème tout entier) reposent sur des fournisseurs de services en ligne et des tiers qui paient des droits ou partagent des recettes pour utiliser le système ou les services des PIMS. De manière générale, les personnes bénéficieraient de services de PIMS gratuits, à l'exception éventuelle de services

supplémentaires fournis directement par l'exploitant du PIMS ou ses partenaires commerciaux.

3. COMMENT LES PIMS PEUVENT-ILS SOUTENIR LES PRINCIPES DE PROTECTION DES DONNÉES?

21 Les PIMS se heurtent à des défis de taille qui les empêchent de se généraliser dans le domaine de la gestion des données à caractère personnel, le marché étant dominé par un nombre limité d'exploitants qui, souvent, n'ont pas intérêt à établir des synergies avec eux[15]. Les PIMS méritent néanmoins d'être soutenus et de faire l'objet d'investissements dans la mesure où ils peuvent appuyer bon nombre des principes, outils et garanties en matière de protection des données qui sont au cœur du nouveau RGPD.

22 Il est essentiel de soutenir ces PIMS qui cherchent réellement à déployer des solutions conformes à la vision et au cadre juridique de l'Union européenne en matière de protection des données. Ce soutien devrait aller de pair avec une application effective des garanties juridiques qui protègent les utilisateurs contre le traitement illicite de leurs données et les techniques intrusives de traçage et de profilage qui visent à contourner les principes fondamentaux de la protection des données.

23 Dans les sections qui suivent, nous examinerons ces principes, ces outils et ces garanties ainsi que les défis à relever.

24 Les questions devant être étudiées portent notamment sur la manière dont les principes de protection des données sont réellement mis en œuvre (par exemple, droits des personnes concernées, mécanismes assurant la validité du consentement, rôle du responsable du traitement et responsabilité, protection des données dès la conception, sécurité); l'interopérabilité et la faisabilité technique; les modèles commerciaux et les intérêts en jeu dans les PIMS; ainsi que la propriété des données à caractère personnel dans le contexte des PIMS.

3.1. Gestion du consentement effectif afin de garantir le contrôle réel par l'utilisateur et le recours à des mécanismes automatiques

25 La gestion du consentement est la fonction centrale des PIMS, qui établissent automatiquement des correspondances entre les préférences de l'utilisateur et les demandes de données à caractère personnel. Il est essentiel de veiller à ce que les préférences en matière de vie privée soient exprimées de manière suffisamment fine et de prendre en considération un contexte complexe d'options possibles. En outre, surtout lorsque la nature des données et le type de traitement sont susceptibles de comporter des risques élevés pour les personnes, il conviendrait d'améliorer leur information contextuelle et d'inclure dans les PIMS des mécanismes destinés à déclencher une intervention humaine. On pourrait examiner s'il serait raisonnable d'exprimer le consentement, moyennant le respect de certaines garanties et conditions à définir, dans des contextes plus vastes tels que les secteurs liés à la recherche médicale.

26 Il importe également que ces mécanismes automatisés soient régulièrement mis en adéquation avec la volonté réelle actuelle de la personne au moyen de rappels ad hoc, afin d'éviter les risques découlant de l'incapacité des personnes à modifier leurs préférences, pour quelque raison que ce soit.

27 L'utilisation de formulaires d'expression des préférences en matière de vie privée lisibles par machine, qui sont transférés en même temps que les données (on parle souvent de «politiques adhésives») ou bien reliés aux données par un lien logique, et le recours à des protocoles permettant leur échange n'ont pas encore fait leur apparition sur le marché. De nouveaux investissements sont nécessaires pour que ces dispositifs s'imposent dans les applications de la vie quotidienne. Plusieurs projets ont été consacrés à cet aspect dans le passé[16]. D'autres évolutions ont suivi, qui méritent d'être prises en considération et analysées plus avant en vue d'un éventuel soutien[17].

28 En particulier, le consentement valide doit être éclairé[18]. Les cadres de confiance qui réglementent le recours aux PIMS par les personnes et les autres parties prenantes (voir la section 2.3) rendent obligatoires la transparence et l'information. Il convient également de noter que, malgré les efforts de recherche sur le recours aux politiques de respect de la vie privée basées sur des procédés automatiques, dans certaines circonstances, les personnes devront encore s'en remettre à leur jugement personnel pour vérifier le niveau et le caractère adéquat des informations fournies.

3.2. Utilisateurs maîtres de leurs données, droits d'accès et de rectification, droit à la portabilité des données, qualité des données

29 L'objectif principal des PIMS est de faire en sorte que les utilisateurs soient maîtres de leurs informations personnelles. Outre leur fonction de mécanisme efficace et convivial permettant de donner ou de retirer le consentement, des PIMS bien conçus pourraient également aider les utilisateurs à exercer leurs droits à accéder à leurs données et à les tenir à jour et exactes, améliorant par là même leur qualité. Les PIMS constituent l'une des initiatives les plus prometteuses pour mettre en œuvre, dès la conception, les droits d'accès et de rectification ainsi que le nouveau droit à la portabilité des données[19]. Ils pourraient également améliorer l'exactitude des données[20] et garantir que leur utilisation sera limitée dans le temps, facilitant ainsi le respect du principe de limitation de la conservation[21].

30 Si la plupart, voire la totalité des PIMS actuels partagent ces objectifs et possèdent des caractéristiques qui leur permettent de les atteindre, cela ne fait pas nécessairement disparaître tout risque de perte de confidentialité et d'utilisation illicite des données. Des mesures techniques peuvent aider à découvrir et prouver les dysfonctionnements, mais si des données quittent un PIMS sous une forme non chiffrée, ou même si des données sont obtenues légalement, puis déchiffrées par une organisation qui ne respecte pas ses obligations, le risque existe que des données soient consultées et utilisées d'une manière non conforme à leur utilisation autorisée telle que configurée dans le PIMS. Ce risque invite à faire preuve de prudence et à vérifier que le traitement déclaré par les PIMS correspond à la réalité.

31 La convivialité des PIMS et la capacité des utilisateurs à obtenir les effets désirés en les utilisant revêtent également une très grande importance, surtout lorsqu'elles sont mises en rapport avec les risques d'exposer des données à caractère personnel, y compris des données sensibles, à la consommation automatique de services en ligne. Les services de PIMS devraient être complétés par un matériel didactique détaillé et par une assistance et une formation graduelles, nonobstant la facilité d'utilisation recherchée. Les fournisseurs et les développeurs devraient envisager un usage éventuel par le grand public, qui ne dispose pas nécessairement des compétences et des connaissances dans les domaines techniques et de la protection des données.

3.3. Protection des données dès la conception et par défaut, interopérabilité

32 Il serait possible d'aider les fournisseurs de services en ligne, qui agissent en qualité de responsables du traitement lorsqu'ils offrent leurs services, à respecter l'obligation de protection des données dès la conception et par défaut en permettant à leurs services d'être reliés aux PIMS en conformité avec les règles de l'UE relatives à la protection des données et en s'assurant que les données à caractère personnel des utilisateurs puissent être exportées facilement et de manière pratique vers les PIMS des personnes. Le recueillement et la gestion du consentement de l'utilisateur, la transparence et la responsabilité, la sécurité lors de l'échange de données ainsi que les mécanismes d'autorisation devraient s'appuyer sur les caractéristiques des PIMS. Cela implique que la responsabilité des exploitants de PIMS de concevoir ces systèmes conformément au RGPD est une question fondamentale. Par conséquent, les décideurs politiques devraient aider les PIMS à concevoir leurs services dans l'objectif spécifique de faciliter le respect du RGPD.

33 L'interopérabilité est une exigence fondamentale, qui doit être satisfaite par les PIMS[22]. Il est nécessaire que l'industrie émergente des PIMS intensifie ses efforts de normalisation et ces efforts devraient être facilités par les décideurs politiques.

3.4. Moyens techniques pour restreindre l'utilisation ultérieure de données à caractère personnel

34 L'application du principe de spécification/limitation du consentement et des finalités et du principe de conservation des données à la mise en adéquation automatique des préférences individuelles avec l'offre en ligne (section 3.1) repose sur la confiance réciproque et la vérification a posteriori si aucune garantie technique adéquate n'est en place. Comme indiqué ci-dessus, certaines solutions[23] font en sorte que ces règles soient automatiquement vérifiées et appliquées, de manière à empêcher l'accès aux données si les règles ne sont pas respectées. La cryptographie aide à vérifier l'identité du consommateur de données ainsi que l'adéquation entre les finalités autorisées et les finalités déclarées et garantit l'intégrité des données et des paramètres utilisés pour en conserver le contrôle. Lorsque, par exemple, un fournisseur de services en ligne veut utiliser des données à caractère personnel, échangées sous une forme chiffrée, à d'autres fins que celles autorisées par l'individu, l'indisponibilité des clés de déchiffrement adéquates l'empêchera d'y accéder[24].

35 Il est impossible de garder le contrôle des données à caractère personnel à l'ère de l'internet des objets et des données massives sans application automatique et fiable, mais contrôlée, des règles relatives à la protection des données. Nous pensons que c'est un des domaines critiques sur lequel les efforts de recherche et d'investissement devraient se focaliser.

3.5. Transparence et traçabilité

36 Touts les traitements de données à caractère personnel n'ont pas pour fondement juridique le consentement. Par exemple, les applications de gouvernement électroniques ont plus de chances de reposer sur une législation européenne ou nationale spécifique ou un autre fondement juridique tel que la nécessité d'exécuter une mission dans l'intérêt public[25]. Même dans ces cas-là, les caractéristiques des PIMS qui permettent de contrôler l'utilisation des données peuvent s'avérer très utiles pour améliorer la transparence et la traçabilité. Les PIMS pourraient, en effet, faciliter l'information des citoyens sur les transferts, conformément à la législation applicable en matière de protection des données.

Par exemple, en consultant leur tableau de bord dans leur PIMS, les citoyens pourraient savoir si leurs données à caractère personnel ont été transférées d'une administration publique à une autre dans les cas où les transferts sont définis par la loi. En outre, même lorsque des données sont traitées pour une finalité spécifique basée sur un autre fondement juridique, les PIMS peuvent aider les personnes à gérer efficacement leur consentement à une utilisation ultérieure éventuelle pour d'autres finalités. Dans ce genre de cas, des mécanismes devraient être conçus pour informer la personne et l'avertir d'un changement éventuel de finalité afin de faciliter le respect des principes de protection des données.

3.6. Sécurité des données

37 Les mécanismes d'identification et d'autorisation des PIMS peuvent tirer parti de la recherche et des évolutions dans d'autres contextes. Des architectures et des solutions d'identification, d'authentification et d'autorisation ouvertes et modulables sont déjà utilisées, et des initiatives sont en cours pour améliorer la technologie. La minimisation des données peut reposer sur le fait que l'authentification est différente de l'identification: une personne n'a pas nécessairement besoin de s'identifier pour être autorisée à accéder à une ressource et à l'utiliser; il suffit, au lieu de cela, de produire une autorisation valide (dont la «validité» est par exemple assurée mutuellement par un tiers jouissant de la confiance des deux parties).

38 Un niveau élevé de sécurité est l'une des caractéristiques nécessaires des PIMS. Comme indiqué précédemment, l'architecture et le recours au chiffrement jouent ici un rôle déterminant. Un chiffrement puissant et sûr devrait toujours être un composant essentiel des PIMS pour que ceux-ci tiennent leurs promesses. La gestion des clés est l'un des facteurs déterminants du chiffrement. Plusieurs modèles sont proposés: les clés de chiffrement peuvent être conservées localement par un appareil de la personne concernée, au niveau du fournisseur de PIMS ou encore par un tiers de confiance. Ces modèles présentent tous des possibilités et des risques différents. Dans tous les cas, la séparation physique des clés et des données est fortement recommandée. L'entreposage centralisé de l'ensemble ou d'une partie très importante des données à caractère personnel d'un utilisateur peut présenter en soi un risque élevé. Quant au lieu de conservation des clés, de nombreux experts en sécurité s'accordent à considérer qu'il peut être risqué d'entreposer des données localement dans des appareils personnels parce qu'ils se caractérisent souvent par un faible niveau de protection. De leur côté, les services en nuage présentent eux aussi des risques spécifiques en matière de sécurité. Dans de nombreuses circonstances, cependant, le fait de confier des données personnelles à un PIMS de confiance, fonctionnant dans un environnement en nuage sûr et bien conçu, pourrait être un choix durable.

39 Les PIMS devraient indiquer clairement à leurs clients les avantages et les risques que leur architecture implique, ainsi que la nature des données qu'ils sont prêts à gérer de manière responsable, afin que les utilisateurs puissent faire un choix éclairé.

3.7. Transferts de données à caractère personnel

40 Les PIMS qui observent les principes de protection des données dès la conception peuvent contribuer à garantir que tout transfert de données à caractère personnel au-delà des frontières de l'Union européenne aura lieu dans le respect des dispositions du RGPD relatives aux transferts internationaux.

41 Les PIMS peuvent aussi contribuer à habiliter les utilisateurs à décider eux-mêmes de l'étendue géographique du partage de leurs données. Selon les spécifications des personnes concernées, les PIMS, tels des portiers, peuvent aider à garantir que les données ne voyageront que dans la mesure où la personne le souhaite.

42 Certaines personnes, par exemple, pourraient ne pas souhaiter que les données concernant leur santé soient transférées en dehors de l'Union européenne (voire au-delà des frontières de leur propre État membre). D'autres pourraient choisir de n'autoriser les transferts que vers les pays censés offrir un niveau adéquat de protection. D'autres encore peuvent être davantage enclins à prendre le risque d'un partage plus large de leurs données. Dans ce cas, les PIMS peuvent également saisir les possibilités supplémentaires que le RGPD leur offre dans le domaine du transfert des données à caractère personnel. Par exemple, ils peuvent conclure des accords de transfert de données avec les destinataires aux termes desquels ces derniers s'engagent à respecter des obligations contractuelles contraignantes conformément à la législation.

3.8. Rôle du responsable du traitement et responsabilité

43 Les PIMS peuvent être considérés comme des intermédiaires ou comme des «plateformes» d'un certain type qui connectent les deux versants du marché: les personnes qui offrent leurs données en vue de leur utilisation ou réutilisation, d'une part, et les organisations qui souhaitent utiliser ou réutiliser celles-ci, d'autre part. Étant donné cette situation particulière, il importe que tout PIMS précise clairement son rôle et sa responsabilité à l'égard des personnes qui lui confient leurs données.

44 En ce qui concerne certains aspects du traitement de données, tels que leur entreposage, il ne fait généralement aucun doute que le PIMS agira en tant que responsable du traitement et qu'il lui incombe par conséquent de les conserver en toute sûreté. Le PIMS devra dès lors être pleinement conforme aux dispositions du RGPD, notamment celles régissant les violations de la sécurité.

45 Dans d'autres cas, l'analyse peut être plus complexe. Il sera, alors, essentiel de clarifier les rôles et les responsabilités[26]. Par exemple, en cas de violation de données ou d'utilisation abusive d'informations par les clients du PIMS (plutôt que par le PIMS lui-même), dans quelle mesure ce dernier sera-t-il responsable? Les PIMS seront-ils responsables du filtrage et de la fiabilité de leurs clients?

46 Il convient en outre de préciser également si les PIMS sont eux-mêmes autorisés à traiter ultérieurement les données et, si tel est le cas, pour quelles finalités et à quelles conditions.

47 Pour tous les aspects, qu'il s'agisse de leurs propres activités de traitement de données ou de celles de leurs clients, il importe également de préciser si les PIMS peuvent limiter contractuellement leur responsabilité, et dans quelle mesure, à l'égard des personnes dont ils détiennent les données (il convient cependant de noter que l'article 82 du RGPD s'appliquera dans tous les cas en ce qui concerne la responsabilité du PIMS en tant que responsable ou responsable conjoint du traitement ou en tant que sous-traitant).

3.9. À la recherche d'un modèle commercial durable dans l'intérêt des personnes

48 Le modèle actuel de recettes sur l'internet repose essentiellement sur la fourniture de services «gratuits» aux personnes en échange de leurs données à caractère personnel. Il est

donc difficile de convaincre un nombre suffisant de personnes de payer pour les PIMS. Dans le même temps, les organisations qui détiennent d'importantes masses de données peuvent avoir tout intérêt à conserver ces données pour elles-mêmes et sous leur contrôle (comme un avantage concurrentiel) plutôt que d'autoriser leur contrôle par les utilisateurs, que ce soit au travers d'un PIMS ou par d'autres moyens (le nouveau droit à la portabilité des données prévu par le RGPD pourrait faire contrepoids à cet égard).

49 Les PIMS peuvent présenter des avantages manifestes pour les fournisseurs de services en ligne. D'un côté, les PIMS peuvent faciliter le respect du RGPD. De l'autre, ils peuvent fournir une série plus complète, plus ciblée et plus propre de données à caractère personnel des consommateurs. Cela réduirait le coût d'accès à ces données.

50 Les modèles commerciaux potentiels pour les PIMS qui pourraient être viables aussi bien pour les personnes que pour les PIMS eux-mêmes comprennent notamment les modèles dits «freemium», qui proposent des fonctions de base gratuites assorties de fonctions supplémentaires payantes, par exemple, l'analyse individuelle en plus des données. Le fait d'offrir l'analyse en tant que service en plus des données et de financer en partie la plateforme de cette façon pourrait constituer en soi un modèle respectueux de la vie privée facilitant l'analyse des données massives en plus des informations personnelles.

Les PIMS peuvent également être proposés en tant que service à des entreprises ou à d'autres organisations soucieuses d'améliorer les services qu'elles offrent à leurs clients par des moyens d'interaction respectueux de leur vie privée. Dans ce contexte, les recettes proviendraient des droits payés par les organisations utilisant les données gérées par les PIMS. De même, les organismes du secteur public peuvent être clients lorsqu'ils envisagent la gestion des informations personnelles afin de permettre aux citoyens de mieux gérer l'accès et l'utilisation de leurs données dans un contexte de «gouvernement électronique», par exemple, lorsque le principe «une fois seulement» est appliqué[27].

51 Par ailleurs, certains effets de l'utilisation des informations personnelles (publicités non sollicitées et similaires, discrimination tarifaire dans le cadre de ventes sur l'internet, autres formes de discrimination ou de refus de service, etc.) peuvent être considérées comme des externalités négatives. Dans ce cas, il est peut-être inéquitable de demander à l'utilisateur de payer en échange d'un plus grand respect de sa vie privée. Le respect de la vie privée est un droit fondamental. Il ne doit pas devenir un privilège réservé aux classes sociales les plus riches.

52 Dans tous les cas, il est essentiel de garantir la transparence du modèle commercial à l'égard des personnes dont les données sont traitées, de manière à ce qu'elles aient conscience des intérêts en jeu (ceux des PIMS et d'autres fournisseurs de services) et qu'elles puissent utiliser les PIMS en toute connaissance de cause.

3.10. «Autoriser l'utilisation» plutôt que la «vente» des données à caractère personnel

53 Le modèle des PIMS semble propice à un débat sur la question de savoir qui «possède» nos données à caractère personnel. Les citoyens de l'Union européenne jouissent d'un droit fondamental à la protection de leurs données à caractère personnel en vertu de l'article 8 de la Charte des droits fondamentaux de l'Union. Les droits et les devoirs précis liés à l'exercice de ce droit sont réglementés plus en détail dans le RGPD récemment adopté. Ces questions ne sont pas propres aux PIMS: les données à caractère personnel sont souvent perçues comme la «rétribution» de services dits «gratuits» sur l'internet. Cette tendance ne

signifie toutefois pas que les données à caractère personnel des personnes peuvent être juridiquement considérées comme un bien susceptible d'être échangé librement de la même manière que n'importe quel autre bien sur le marché. Au contraire, les PIMS ne seront en principe pas en mesure de «vendre» des données à caractère personnel. Leur rôle sera plutôt d'autoriser des tiers à utiliser ces données pour des finalités et des durées spécifiques, moyennant le respect de certaines conditions définies par les personnes elles-mêmes et de toutes les autres sauvegardes prévues par la législation applicable en matière de protection des données.

4. CONCLUSIONS ET PROCHAINES ÉTAPES

4.1 Vers une application intégrale du RGPD - Perspectives

54 Comme indiqué ci-dessus, le législateur de l'Union européenne a adopté récemment un train de réformes sur la protection des données qui renforce et modernise le cadre réglementaire de manière à ce qu'il reste efficace à l'ère des données massives.

55 Le nouveau RGPD, qui comprend des règles relatives à une transparence accrue, à des droits d'accès puissants et à la portabilité des données, devrait contribuer à donner aux personnes un plus grand contrôle sur leurs données. Il pourrait aussi contribuer à des marchés plus efficaces pour les données à caractère personnel, dans l'intérêt des consommateurs comme dans celui des entreprises.

56 Les codes de conduite et les systèmes de certification prévus par le RGPD constituent des instruments privilégiés pour donner une visibilité et un rôle spécifiques aux technologies et aux produits qui – comme les PIMS – peuvent contribuer à une application plus efficace de la législation relative à la protection des données sur le plan pratique.

57 Les PIMS se heurtent toutefois à une difficulté générale: ils doivent pénétrer un marché dominé par des services en ligne qui reposent sur des modèles commerciaux et des architectures techniques où les personnes ne contrôlent pas leurs données, comme expliqué à la section 3.9. Le passage à une situation où les personnes ont la possibilité réelle d'accorder à un fournisseur de services l'accès à certaines données dans leur PIMS au lieu de les lui fournir directement nécessitera des mesures incitatives supplémentaires à l'intention des fournisseurs de services. La Commission peut mettre à profit les initiatives qu'elle a annoncées sur les flux et la propriété des données[28] pour envisager des initiatives politiques supplémentaires qui pourraient inciter les responsables du traitement à accepter cette manière de fournir des données. En outre, une initiative des services publics de gouvernement électronique visant à accepter les PIMS comme source de données en remplacement de la collecte directe de données pourrait favoriser l'acceptation des PIMS.

58 Cette analyse pourrait être complétée par des mesures visant à jeter les fondements techniques, sociétaux et économiques, notamment des efforts de normalisation et des incitations économiques et à encourager des projets pilotes et de recherche.

59 C'est en premier lieu dans le cadre des administrations publiques de l'Union européenne et des États membres et des projets cofinancés par eux que ce changement de perspective devrait être éprouvé, encouragé et, si tout va bien, réalisé.

4.2 Soutenir les PIMS et la technologie sous-jacente pour une protection efficace des données

60 Une bonne réglementation, même si elle est essentielle, n'est pas en soi suffisante. Comme nous l'avons affirmé dans notre avis intitulé «Relever les défis des données massives»[29], les entreprises et les autres organisations qui déploient d'importants efforts dans la recherche de solutions innovantes pour l'utilisation des données à caractère personnel devraient faire preuve du même esprit innovant dans la mise en œuvre des principes de protection des données.

61 La contribution de la technologie au modèle des PIMS est fondamentale. Les PIMS peuvent servir à éprouver les approches basées sur la protection des données dès la conception et les technologies qui les sous-tendent. Les thèmes de recherche pertinents, qui nécessiteront un soutien et des investissements adéquats, sont notamment les suivants: la gestion des identités interopérable et respectueuse de la vie privée; les mécanismes d'autorisation; l'interopérabilité des données; la sécurité des données; ainsi que les mécanismes d'exécution automatique de «contrats» établis entre les personnes et d'autres parties. Ces thèmes seront favorisés par le chiffrement et la cryptographie et alimentés par la disponibilité d'une capacité informatique peu onéreuse. Il est nécessaire que les décideurs politiques, tels que la Commission, apportent un soutien décisif à la recherche fondamentale et à la recherche appliquée dans ces domaines technologiques à ce stade initial de manière à ne pas gaspiller les possibilités actuelles.

62 Afin d'encourager la recherche et le développement et le déploiement vers le marché dans le domaine des PIMS, nous recommandons à la Commission d'envisager des synergies éventuelles avec d'autres domaines de la stratégie pour un marché unique numérique, tels que l'informatique en nuage et l'internet des objets. Ainsi, des projets pilotes pourraient être mis en œuvre pour concevoir et expérimenter les interactions entre les services en nuage et l'internet des objets, d'une part, et les PIMS, d'autre part.

4.3 Comment le CEPD fera-t-il avancer ce débat?

63 Le CEPD entend contribuer à encourager les efforts des secteurs privé et public dans le sens décrit ci-dessus. Il continuera à faciliter les discussions, notamment par l'organisation d'événements et d'ateliers, par exemple, pour mettre en évidence, encourager et promouvoir les bonnes pratiques visant à accroître la transparence et le contrôle par les utilisateurs et à étudier les possibilités offertes par les PIMS. Il continuera également à faciliter les travaux du réseau d'ingénierie de la vie privée sur l'internet (IPEN) en tant que centre de connaissances interdisciplinaires pour les ingénieurs et les spécialistes de la vie privée. Dans ce contexte, il continuera à offrir une plateforme aux développeurs et aux promoteurs de PIMS pour leur permettre de communiquer avec des spécialistes d'autres technologies et de la protection des données.

Marrakech, le 20 octobre 2016

(**signature**)

Giovanni Buttarelli
Contrôleur européen de la protection des données

Notes

[1] Communication COM(2014)442 relative à une économie de la donnée prospère: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy.
[2] Avis nº 7/2015 du CEPD: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_FR.pdf . Voir en particulier la section 3.
[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données); JO L 119 du 4.5.2016, disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2016:119:FULL.
[4] Voir entre autres l'article 6, paragraphe 1, point a), les articles 7 et 8 et les considérants 42 et 43 du RGPD.
[5] Article 25 du RGPD.
[6] Article 20 du RGPD.
[7] Parmi les concepts connexes figurent les «entrepôts de données personnelles», les «espaces de données personnelles» et les «coffres de données personnelles». Le terme «PIMS» sera utilisé dans le présent avis étant donné qu'il décrit le mieux le concept d'une manière générale et aisément compréhensible. Tel qu'il est utilisé dans le présent avis, l'acronyme «PIMS» est soit au singulier, soit au pluriel – système ou systèmes de gestion des informations personnelles.
[8] Voir le considérant 7 du RGPD: «Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant». Voir aussi, par exemple, Doc Searls, *The Intention Economy: When Customers Take Charge* (Boston: Harvard Business Review Press, 2012).
[9] Voir, par exemple, Ira S. Rubinstein, *Big Data*: *The End of Privacy or a New Beginning?* International Data Privacy Law, 2013, vol. 3, nº 2.
[10] Voir, par exemple, le rapport sur les entrepôts de données personnelles rédigé par l'université de Cambridge à la demande de la Commission européenne: https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school.
[11] Voir entre autres: Kai Rannenberg, Jan Camenisch, Ahmad Sabouri (éd.), *Attribute-based credentials for trust*, (Cham: Springer International Publishing, 2015).
[12] Pour de plus amples informations sur le concept d'anonymisation et son efficacité, voir aussi l'avis 05/2014 du groupe de travail «Article 29» sur les techniques d'anonymisation: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[13] Voir, par exemple, le projet openPDS: http://openpds.media.mit.edu/.
[14] Voir par exemple la fondation Qiy (https://www.qiyfoundation.org/) et le réseau Respect (https://www.respectnetwork.com/ et http://oixnet.org/registry/respect-network/).
[15] Voir l'avis préliminaire du CEPD intitulé «Vie privée et compétitivité à l'ère de la collecte de données massives». https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_FR.pdf. Voir en particulier la section 4.2.2: *«Des entreprises puissantes ou dominantes sont en mesure d'exploiter des "économies d'agrégation" et de créer des barrières à l'entrée du fait de leur contrôle d'ensembles volumineux de données à caractère personnel associés à des logiciels propriétaires qui organisent les données».*
[16] Une initiative bien connue est le projet P3P W3C et APPEL, le langage d'échange des préférences pertinentes.
[17] Voir par exemple l'initiative Kantara (https://kantarainitiative.org/), sous l'égide de laquelle de nombreux projets sont réalisés dans le but de favoriser un «accès sûr et respectueux de la vie privée à des services en ligne dignes de confiance».
[18] Article 4, paragraphe 11, du RGPD.
[19] Voir l'article 20 du RGPD.
[20] Article 5, paragraphe 1, point d), du RGPD.
[21] Article 5, paragraphe 1, point e), du RGPD.
[22] Un exemple notoire est l'utilisation de la suite de protocoles XDI proposée par l'organisation d'intérêt public XDI (http://xdi.org/), qui permet d'échanger en toute sécurité et en toute confiance des données en fonction de critères définis (par exemple, des préférences en matière de vie privée).
[23] Un exemple de ce genre de solution est fourni par les «contrats intelligents», qui prévoient la négociation et l'exécution automatisées du contrat. Le concept remonte aux années 1990, époque à laquelle il a été inventé

par le cryptographe Nick Szabo (http://szabo.best.vwh.net/smart_contracts_idea.html). Il a récemment suscité un nouvel élan dans la recherche à la suite de l'évolution de la cryptographie.

[24] Habituellement, cela est également possible grâce à l'intervention des fournisseurs d'identité/d'authentification, qui jouissent de la confiance de l'ensemble des parties concernées et garantissent l'authenticité des «attributs» des données (préférences en matière de vie privée et autres éléments d'information) et des finalités/utilisations des données affichées par les services en ligne, ainsi que l'identité de ces services. En outre, des mesures peuvent être prises lors de certains événements, comme la réussite ou l'échec du déchiffrage tel que les notifications de l'événement au PIMS, qui permet le contrôle.

[25] Article 6, paragraphe 1, points c) et e), du RGPD.

[26] Voir aussi l'article 82 du RGPD.

[27] Il s'agit là du principe selon lequel les citoyens devraient être invités par l'autorité publique à soumettre une information ou un document donné une fois seulement dans un contexte où les autorités publiques sont ensuite invitées à partager l'information ou le document. Il peut apparaître souhaitable de prévoir l'entreposage de ces informations sur la plateforme d'un PIMS afin de renforcer la transparence et de donner aux personnes une meilleure maîtrise de leurs données.

[28] Communication: Passage au numérique des entreprises européennes –Tirer tous les avantages du marché unique numérique http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm.

[29] Avis nº 7/2015 du CEPD, cité ci-dessus.