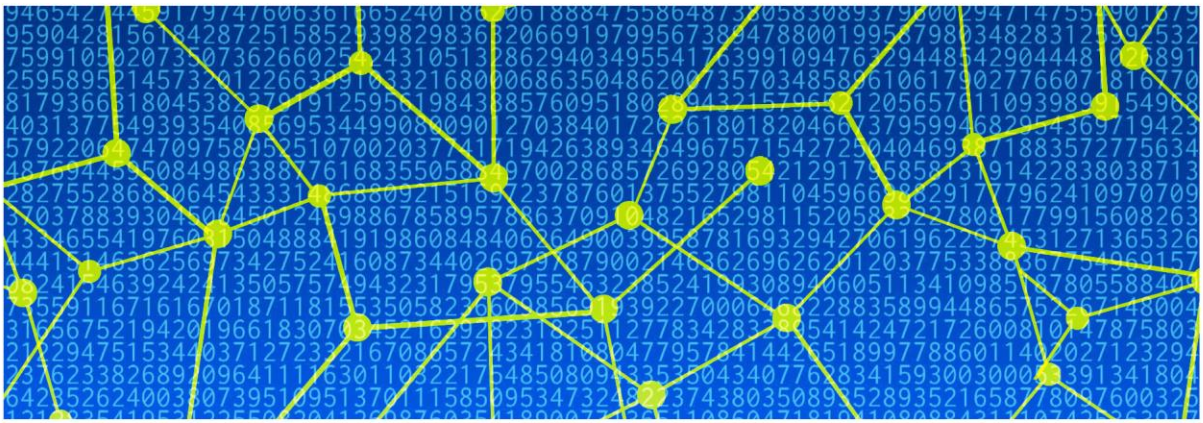

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 8/2017

Avis du CEPD sur la proposition de règlement établissant un portail numérique unique et sur le principe «une fois pour toutes»

EDPS

1er août 2017

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE 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, la Commission a l'obligation, «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…», 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 répond à une consultation formelle de la Commission européenne au titre de l'article 28, paragraphe 2, du règlement n° 45/2001 ainsi qu'à une consultation concomitante du Parlement européen, et formule des observations et des recommandations sur la manière de mieux protéger le droit au respect de la vie privée et la protection des données à caractère personnel dans la proposition de règlement établissant un portail numérique unique et modifiant le règlement IMI (1024/2012).

Synthèse

La proposition est l'un des premiers instruments de l'UE à faire explicitement référence au principe «*une fois pour toutes*», qui tend à ce que les citoyens et les entreprises soient invités à ne fournir qu'une seule fois les mêmes informations à une administration publique, laquelle peut ensuite réutiliser les informations dont elle dispose déjà. La proposition prévoit que l'échange de justificatifs pour certaines procédures transfrontières particulières (comme une demande de reconnaissance de diplôme) soit déclenché par la demande expresse d'un utilisateur et que la procédure se déroule dans le cadre d'un système technique mis en place par la Commission et les États membres et assorti d'un mécanisme intégré de prévisualisation assurant la transparence vis-à-vis de l'utilisateur.

Le CEPD se félicite de la proposition de la Commission de moderniser les services administratifs et apprécie que cette dernière se préoccupe de l'impact de sa proposition sur la protection des données à caractère personnel. Le présent avis est formulé à la demande spécifique de la Commission et du Parlement. Il s'inspire également des priorités fixées par la Présidence estonienne du Conseil, qui incluent spécifiquement «*une Europe numérique et la libre circulation des données*».

En plus de formuler des recommandations spécifiques visant à poursuivre l'amélioration qualitative de la législation, le CEPD tient également à saisir cette occasion pour donner un premier aperçu des questions clés liées au principe «une fois pour toutes» en général, bien qu'un grand nombre d'entre elles ne découlent pas nécessairement de la proposition sous sa forme actuelle. Ces questions concernent, en particulier, la base juridique du traitement, la limitation de la finalité et les droits de la personne concernée. Le CEPD insiste sur le fait que pour assurer une mise en œuvre réussie du principe «une fois pour toutes» et permettre un échange transfrontière licite des données, ledit principe doit être appliqué conformément aux principes pertinents de la protection des données.

S'agissant de la proposition proprement dite, le CEPD soutient les efforts déployés pour s'assurer que les citoyens gardent le contrôle des données à caractère personnel les concernant, notamment en exigeant «*une demande expresse de l'utilisateur*» avant tout transfert de justificatifs entre autorités compétentes et en offrant à l'utilisateur la possibilité de «*visualiser le justificatif avant l'échange*». Il se réjouit également des modifications apportées au règlement IMI, qui confirment et actualisent les dispositions relatives au mécanisme de supervision coordonnée prévu pour le système d'information du marché intérieur («*IMI*») et permettraient également au comité européen de la protection des données de mettre à profit les possibilités techniques de l'IMI pour échanger des informations dans le cadre du règlement général sur la protection des données (RGPD).

Cet avis énonce des recommandations sur une série de questions, en insistant sur la base juridique de l'échange transfrontière de justificatifs, la limitation de la finalité et le champ d'application du principe «une fois pour toutes», ainsi que des préoccupations pratiques concernant le contrôle par l'utilisateur. Les recommandations principales précisent notamment que la proposition ne contient pas de base juridique pour l'utilisation du système technique en vue d'échanger des informations à des fins autres que celles prévues dans les quatre directives citées ou prévues par ailleurs dans le droit national ou de l'UE applicable et que la proposition n'a pas pour but de restreindre le principe de la limitation de la finalité au titre du RGPD; elles clarifient également une série de points en rapport avec la mise en œuvre du contrôle par l'utilisateur. S'agissant des modifications du règlement IMI, le CEPD recommande d'ajouter

le RGPD à l'annexe du règlement IMI afin de permettre l'utilisation potentielle de l'IMI aux fins de la protection des données.

TABLE DES MATIÈRES

I. Table des matières

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la 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[1], et vu le 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)[2],

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[3], et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

Le 2 mai 2017, la Commission européenne («*la Commission*») a adopté une proposition de règlement du Parlement européen et du Conseil établissant un programme numérique unique pour donner accès à des informations, des procédures et des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) nº 1024/2012[4] («*la proposition*»).

La proposition vise à faciliter les activités transfrontières des citoyens et des entreprises en leur donnant, par le biais d'un portail numérique unique, un accès convivial aux informations, aux procédures et aux services d'assistance et de résolution de problèmes dont ils ont besoin pour exercer leurs droits dans le marché intérieur. Sous cet angle, cette proposition représente une initiative importante de la Commission pour réaliser un marché intérieur plus approfondi et plus équitable et développer un marché unique numérique[5].

Les articles 4 à 6 de la proposition décrivent brièvement les «services proposés par le portail» qu'offre le portail numérique unique. Ils reflètent étroitement l'intitulé de la proposition proprement dite et incluent:

- l'accès aux informations,
- l'accès aux procédures et
- l'accès aux services d'assistance et de résolution de problèmes.

Il est également à noter que la proposition, en son article 36, tend à modifier plusieurs dispositions du règlement (UE) nº 1024/2012 («*règlement IMI*»)[6], qui établit la base juridique du fonctionnement du système d'information du marché intérieur («*IMI*»)[7].

La proposition est l'un des premiers instruments de l'UE qui fait explicitement référence au principe «une fois pour toutes» et qui le met en œuvre[8]. Elle fait référence à la notion «une fois pour toutes» et à ses avantages en expliquant que les «*citoyens et les entreprises ne devraient pas être tenus de fournir les mêmes informations à des autorités publiques plus d'une fois dans le contexte de l'échange transfrontière de justificatifs*»[9]. La proposition prévoit que l'échange

de justificatifs pour certaines procédures soit déclenché par la demande d'un utilisateur et passe par le système technique mis en place par la Commission et les États membres[10] (pour plus de détails, voir la section 3 ci-dessous).

Le présent avis répond à une demande de la Commission et à une demande ultérieure distincte du Parlement européen («*le Parlement*») adressées au Contrôleur européen de la protection des données («*CEPD*»), en tant qu'autorité de contrôle indépendante, de présenter un avis sur la proposition. Le CEPD se réjouit d'avoir été consulté par les deux institutions. Le présent avis fait suite à une consultation informelle du CEPD par la Commission avant l'adoption de la proposition.

Le CEPD en prend note et se félicite de la proposition de la Commission de moderniser les services administratifs en améliorant la disponibilité, la qualité et l'accessibilité des informations dans l'Union européenne. Il insiste aussi tout particulièrement sur le fait que le principe «une fois pour toutes » pourrait contribuer à la réalisation de ces objectifs, sous réserve du respect de la législation applicable en matière de protection des données et du respect des droits fondamentaux des personnes.

Le CEPD apprécie que la Commission et le Parlement se préoccupent de l'impact que la présente proposition pourrait avoir sur la protection des données à caractère personnel. Il se réjouit que bon nombre de ses commentaires informels aient été pris en considération. Il soutient tout particulièrement:

- les efforts déployés pour s'assurer que les personnes gardent le contrôle des données à caractère personnel les concernant, notamment en exigeant «*une demande expresse de l'utilisateur*» avant tout transfert de preuve entre autorités compétentes (article 12, paragraphes 2 et 4) et en offrant à l'utilisateur la possibilité de «*visualiser le justificatif avant l'échange*» (article 12, paragraphe 2, point e));
- les efforts déployés pour définir le champ d'application matériel du principe «une fois pour toutes» (article 12, paragraphe 1);
- l'exigence expresse d'utiliser des données anonymisées et/ou agrégées pour la collecte des statistiques et des avis des utilisateurs pertinents (articles 21 à 23);
- il se félicite en outre de la modification proposée au règlement IMI, qui confirme et actualise les dispositions relatives au mécanisme de surveillance coordonnée de l'IMI en vue d'assurer une approche cohérente (article 36, paragraphe 6, point b));
- enfin, sont également accueillies favorablement, les dispositions plus générales marquant l'engagement de veiller au respect des droits fondamentaux des personnes, notamment le droit à la protection des données à caractère personnel, tels que ceux visés aux considérants 43 et 44 et à l'article 29.

Le présent avis a pour but de formuler des recommandations spécifiques afin de lever les dernières préoccupations liées à la protection des données et d'améliorer ainsi davantage la qualité de la législation (voir la section 3 ci-dessous). Parmi les trois services proposés par le portail énumérés plus haut, le présent avis se concentrera sur l'«*accès aux procédures*» (article 5) et, notamment, sur les dispositions relatives à l'«*échange transfrontière de justificatifs entre autorités compétentes*» visé à l'article 12, étant donné qu'elles sont les plus pertinentes pour la protection des données à caractère personnel. Le reste de la proposition (y compris ses dispositions sur l'accès à l'information et l'accès aux services d'assistance et de résolution de problèmes) soulève moins de préoccupations en termes de protection des données. Par ailleurs, le CEPD commente également brièvement certaines modifications proposées au règlement IMI.

En outre, le CEPD tient également à profiter de cette occasion pour donner un premier aperçu des questions clés liées au principe «une fois pour toutes» en général, bien qu'un grand nombre d'entre elles ne découlent pas nécessairement de la proposition sous sa forme actuelle (voir la section 2 ci-dessous).

2. LE PRINCIPE «UNE FOIS POUR TOUTES» ET LA PROTECTION DES DONNÉES

Il n'existe pas de définition communément admise du principe «une fois pour toutes». Il peut, en effet, être mis en œuvre de différentes manières et à des degrés divers[11]. De façon générale, le principe «une fois pour toutes» implique un échange d'informations ou de documents (automatiquement ou sur demande) entre différents ministères aux fins d'exercer leurs missions d'intérêt public. L'objectif est de réduire les charges administratives, de faciliter la réutilisation de l'information et de contribuer à éviter - comme le nom l'indique - que les personnes physiques et les entreprises ne doivent fournir plus d'une fois les mêmes documents ou informations au gouvernement.

Le principe «une fois pour toutes» dans le plan d'action européen 2016-2020 pour l'administration en ligne: les bénéfices potentiels

Le plan d'action européen 2016-2020 pour l'administration en ligne reconnaît que permettre aux administrations publiques d'accéder aux données «*accroîtra l'efficacité [de ces administrations] et facilitera la libre circulation, pour les citoyens comme pour les entreprises*»[12]. Une étude préparée pour la Commission et intitulée *EU-wide digital Once-Only Principle for citizens and businesses* («étude Smart») confirme cette affirmation et reconnaît qu'une application du principe «une fois pour toutes» à l'échelle de l'Union pourrait offrir des avantages considérables à l'administration publique, aux personnes physiques et aux entreprises[13]. Elle explique, en outre, que l'application de ce principe à toute l'Union européenne pourrait répondre aux attentes des non-ressortissants de bénéficier de certains services sans être soumis à des charges administratives inutiles[14].

Le plan d'action 2016-2020 pour l'administration en ligne susvisé décrit comme suit le principe «une fois pour toutes»: *« les administrations publiques devraient veiller à ce que les citoyens et les entreprises ne doivent communiquer une même information qu'une seule fois à une administration donnée*»[15]. Les gouvernements ne demanderont donc plus « *plusieurs fois la même information lorsqu'ils peuvent utiliser celles dont ils disposent déjà*»[16] et aucune charge supplémentaire ne pèsera sur les citoyens et les entreprises[17]. Fondamentalement, cela signifie que les autorités compétentes seraient autorisées à échanger et à utiliser (effectuer un traitement ultérieur) – ou seraient effectivement tenues de le faire – des données (y compris des données à caractère personnel) dans un contexte différent et pour une finalité différence de celle visée lorsque les données ont été initialement collectées. L'étude Smart reconnaît que le principe «une fois pour toutes» «*dépend de la compréhension et de l'acceptation collectives de la réutilisation des données*»[18].

Aspects liés à la protection des données

Le principe «une fois pour toutes» – selon la définition qui en est donnée et la manière dont il est mis en œuvre – peut potentiellement soulever des problèmes en termes de protection des données à caractère personnel, notamment en ce qui concerne:

- la base juridique du traitement,
- la limitation de la finalité et la minimisation des données
- et les droits des personnes concernées.

Le CEPD insiste sur le fait que pour assurer une mise en œuvre réussie du principe «une fois pour toutes» à l'échelle de l'UE et permettre un échange transfrontière licite des données, ledit principe doit être appliqué conformément aux principes pertinents de la protection des données[19]. Quelques-unes des questions clés liées à la protection des données sont mentionnées ci-dessous.

La base juridique du traitement

L'article 6 du règlement général relatif à la protection des données («*RGPD*»)[20] prévoit que les données à caractère personnel ne sont traitées que si au moins un des fondements juridiques énumérés dans ledit article s'applique. Cette exigence est liée au principe plus large de la «*licéité*» du traitement visé à l'article 5, paragraphe 1, point a), qui impose que les données à caractère personnel soient traitées «de manière licite». Les trois fondements juridiques les plus pertinents pour la mise en œuvre du principe «une fois pour toutes» sont le consentement[21], l'obligation légale[22] et l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique[23].

En fonction des circonstances, l'une ou l'autre de ces bases juridiques pourrait constituer le choix le plus adéquat. Les sous-sections qui suivent présentent un rapide aperçu de chacun des fondements juridiques et quelques exemples pratiques.

En règle générale, dans le cas de tout partage de données structurelles et récurrentes, aux fins de garantir la sécurité juridique, le CEPD recommande que, dans toute la mesure du possible, le traitement ultérieur de données à caractère personnel basé sur le principe «une fois pour toutes» soit spécifié dans un instrument législatif offrant des garanties adéquates pour assurer le respect de la législation en matière de protection des données, notamment le principe de limitation de la finalité et le respect des droits des personnes concernées[24].

L'instrument législatif qui introduit l'application du principe «une fois pour toutes» devrait indiquer clairement si l'échange de données gouvernementales est soumis au consentement libre, spécifique, éclairé et univoque des personnes concernées ou si la loi crée une obligation ou une autorisation de partage des données.

Afin de garantir la sécurité juridique, normalement, il est également utile que la loi précise clairement la base juridique du traitement de données à caractère personnel (généralement dans le texte même de l'instrument juridique ou dans un considérant, lorsque cette approche est suffisante et adéquate).

Consentement

S'il est utilisé de manière adéquate, le consentement peut apporter aux personnes concernées un bon niveau de contrôle de leurs données. Cependant, il faut pour cela que le consentement réponde aux exigences du RGPD; en d'autres termes, il doit être libre, spécifique, éclairé et univoque. Ces exigences ont été développées par le groupe de travail «Article 29» dans son avis 15/2011 sur la définition du consentement[25] et précisées davantage dans le RGPD.

L'une des conditions pour qu'un consentement soit valable est qu'il soit donné librement[26]. Le RGPD dispose qu'un consentement ne peut pas être considéré comme donné librement - et donc licite - lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement.

Bien que chaque situation doive être appréciée individuellement, un tel déséquilibre est probable lorsque le responsable du traitement est une autorité publique[27]. Si le principe «une fois pour toutes» devait reposer sur le consentement de la personne concernée, des garanties suffisantes devraient être mises en place pour s'assurer que le consentement soit donné librement. Un consentement ne peut être «contraint».

Obligation légale

Un responsable du traitement peut se fonder sur la base juridique de l'obligation légale lorsque «*le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis*»[28]. Cette base juridique peut être invoquée tant par des entités publiques que privées lorsque l'obligation de traiter des données à caractère personnel est imposée par la loi[29].

Elle ne peut pas être utilisée comme base juridique lorsque la loi permet uniquement un traitement, mais ne l'exige pas. En outre, comme expliqué par le groupe de travail «Article 29» dans son avis 6/2014 sur l'intérêt légitime[30], la loi imposant l'obligation légale doit remplir «*toutes les conditions requises pour rendre l'obligation valable et contraignante, et doit aussi être conforme au droit applicable en matière de protection des données, notamment aux principes de nécessité, de proportionnalité et de limitation de la finalité*»[31]. De plus, pour pouvoir invoquer cette base juridique, le responsable du traitement ne peut avoir «*de marge d'appréciation injustifiée quant à la façon de se conformer à l'obligation légale*»[32].

Le considérant 45 du RGPD énonce d'autres conditions pour que la loi puisse imposer l'obligation. La loi doit, notamment, préciser les finalités du traitement et établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et «*d'autres mesures visant à garantir un traitement licite et loyal*».

En conclusion, l'utilisation adéquate de la base juridique de l'obligation légale contribue à la sécurité juridique du traitement de données à caractère personnel et peut dès lors constituer une base juridique adéquate dans de nombreuses situations impliquant un partage de données entre autorités publiques, en particulier lorsque les risques en termes de protection des données à caractère personnel sont élevés. Dans le même temps, il convient de garder à l'esprit les limites de cette base juridique: elle est moins flexible et peut donc limiter la capacité du responsable du traitement à choisir et à optimiser le traitement en fonction des circonstances particulières. De plus, elle ne peut être invoquée dans les cas où le responsable du traitement est autorisé à partager des données à caractère personnel, mais n'y est pas tenu.

Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Enfin, l'article 6, paragraphe 1, point e), prévoit qu'un responsable du traitement peut traiter des données à caractère personnel lorsque «*le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement*». Un responsable du traitement ne peut se prévaloir de cette base juridique que si le droit de l'Union ou d'un État membre énonce la mission d'intérêt public[33].

Cette base juridique est très semblable à celle de l'obligation légale discutée plus haut. En effet, les exigences spécifiques du considérant 45 du RGPD résumées plus haut lui sont également applicables. Par conséquent, dans la pratique, cette base juridique requiert également des circonstances très spécifiques, tout en offrant un peu plus de flexibilité à l'organisation qui traite les données.

En outre, à la différence de la base juridique de l'obligation légale, la loi peut donner une certaine marge d'appréciation au responsable du traitement pour décider s'il partage ou non les données et peut donc s'appliquer lorsque la loi autorise mais n'impose pas de partager les données[34]. De plus, une garantie supplémentaire importante est constituée par le fait que – tout comme pour le traitement fondé sur un intérêt légitime – les personnes concernées ont le droit de s'opposer à un traitement basé sur ce fondement juridique[35].

Limitation de la finalité

Afin de se conformer au principe de limitation de la finalité, l'article 5, paragraphe 1, point b), du RGPD, impose que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes, et ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités.

Pour appliquer ce principe (sous réserve de quelques exceptions notables qui seront discutées plus avant), l'article 6, paragraphe 4, du RGPD dispose que les différentes finalités pour lesquelles les données à caractère personnel doivent être traitées devraient être appréciées à la lumière de la finalité pour laquelle les données ont été initialement collectées afin de garantir la compatibilité. L'article 6, paragraphe 4, énumère les facteurs suivants qui doivent, entre autres, être pris en compte lors de l'appréciation de la compatibilité:

- l'existence d'un lien entre la finalité initiale et la finalité ultérieure,
- le contexte de la collecte, en particulier la relation entre la personne concernée et le responsable du traitement,
- la nature des données (en particulier si le traitement porte sur des catégories particulières de données),
- les conséquences possibles pour les personnes concernées et
- l'existence de garanties (comme le chiffrement ou la pseudonymisation)[36].

Le RGPD introduit une nouveauté: l'article 6, paragraphe 4, codifie également une exception au principe de limitation de la finalité lorsque le traitement ultérieur repose sur le consentement ou sur le droit de l'Union ou d'un État membre[37].

Il ne s'agit toutefois pas d'une autorisation illimitée d'adopter tout texte législatif général et large permettant de réutiliser sans fin des données à caractère personnel entre différents ministères. Conformément à la Charte des droits fondamentaux, la loi doit respecter certaines exigences pour qu'il puisse être dérogé au principe de limitation de la finalité.

En particulier, elle doit constituer *«une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1*». Ces objectifs couvrent la sécurité nationale, la défense, la lutte contre la criminalité et d'autres objectifs spécifiquement mentionnés d'intérêt public.

Certains de ces objectifs d'intérêt public peuvent être pertinents pour certaines applications spécifiques et ciblées du principe «une fois pour toutes» (par exemple, certaines mesures nécessaires et proportionnées pour lutter contre la criminalité au titre de l'article 23,

paragraphe 1, point d) ou en lien avec la perception des impôts en vertu du point e) de la même disposition).

L'allégement de la charge administrative sur les personnes physiques ou les organisations, l'efficacité accrue des procédures administratives et l'économie de temps et de ressources, qui sont souvent les objectifs premiers des applications du principe «une fois pour toutes» constituent sans nul doute des objectifs d'intérêt public valables. Néanmoins, ils ne sont pas spécifiquement mentionnés dans la liste visée à l'article 23, paragraphe 1, et ne constituent pas en soi un motif licite permettant de restreindre la portée du principe de limitation de la finalité pour atteindre ces objectifs. Cela étant, comme indiqué plus haut, on ne peut exclure que dans certains cas spécifiques, l'un ou l'autre des fondements juridiques des limitations visées à l'article 23, paragraphe 1, point d), puisse être approprié.

En conclusion, conformément aux observations qui précèdent et à moins qu'un motif approprié de limitation visé à l'article 23, paragraphe 1, soit disponible ou que les personnes concernées aient donné leur consentement, le principe de limitation de la finalité doit être respecté, même lorsqu'une législation de l'Union ou d'un État membre prévoit l'application du principe «une fois pour toutes».

Contrôle par l'utilisateur, transparence et systèmes de gestion des informations personnelles (PIMS)

Dans son avis «*Relever les défis des données massives*»[38], le CEPD a déclaré que la transparence et le contrôle par l'utilisateur devraient contribuer à faire en sorte que les personnes concernées puissent s'opposer à une utilisation abusive et empêcher l'utilisation secondaire de données à des fins qui ne répondent pas à leurs attentes légitimes.

Ces considérations valent également pour le partage de données entre autorités publiques lorsque le principe «une fois pour toutes» est appliqué. En effet, dans son avis 9/2016 du 20 octobre 2016 sur les systèmes de gestion des informations personnelles (PIMS)[39], le CEPD a expliqué que les caractéristiques des systèmes de gestion des informations qui permettent un contrôle par l'utilisateur peuvent se révéler très utiles pour accroître la transparence et la traçabilité. L'avis soulignait plus particulièrement que les organismes du secteur public peuvent exploiter ces caractéristiques afin de permettre aux citoyens de mieux gérer l'accès et l'utilisation de leurs données.

Ces caractéristiques pourraient permettre d'informer plus facilement les personnes concernées au sujet de l'échange de données entre autorités publiques. Par exemple, en consultant leur tableau de bord dans leur PIMS (et/ou en recevant une alerte sur leur smartphone), les personnes concernées pourraient savoir si leurs données à caractère personnel ont été transférées d'une administration publique vers une autre, dans les cas où les transferts sont définis par la loi. Les PIMS peuvent également aider les citoyens à gérer efficacement leur consentement en vue d'une possible utilisation ultérieure dans les cas où leur consentement est requis pour une telle utilisation.

Enfin, l'avis suggérait qu'une initiative des services publics d'administration en ligne visant à accepter les PIMS comme source de données en remplacement de la collecte directe de données pourrait favoriser l'acceptation des PIMS.

Minimisation des données et autres principes de la protection des données

Outre les questions mises en évidence ci-dessus, l'application licite du principe «une fois pour toutes» doit également respecter les autres principes régissant la protection des données, notamment ceux d'équité, de transparence[40], de minimisation des données, d'exactitude, de limitation de la durée de conservation, d'intégrité et de confidentialité[41], ainsi que la protection des données dès la conception et par défaut[42]. Conformément au principe de responsabilité, les autorités compétentes doivent être en mesure de prouver le respect des principes susvisés[43].

L'étude Smart a, par exemple, observé que les autorités publiques recueillent un tas de données inutiles parce qu'elles étaient utilisées à une fin particulière dans le passé[44]. Une telle pratique n'est conforme ni avec le principe de limitation de la finalité ni avec celui de la minimisation des données et devrait être revue avant toute application du principe «une fois pour toutes».

3. RECOMMANDATIONS

Ainsi que cela a été observé à la section 1, le CEPD se félicite des efforts déployés pour tenir compte des préoccupations relative à la protection des données lors de la rédaction de la proposition. Dans le même temps, afin d'améliorer encore la qualité de la proposition législative, d'accroître la sécurité juridique et de renforcer la transparence et le contrôle par l'utilisateur, le CEPD formule quelques recommandations supplémentaires concernant l'échange de justificatifs, en particulier, sur les points suivants:

- la base juridique de l'échange de justificatifs (article 12, paragraphe 1);
- la limitation de la finalité;
- la notion de demande expresse (article 12, paragraphe 4);
- la notion de prévisualisation et ses conséquences (article 12, paragraphe 2, point e));
- la définition du justificatif et l'éventail de procédures en ligne couvertes (article 3, paragraphe 4, et article 2, paragraphe 2, point b)).

Les recommandations du présent avis se concentreront sur les dispositions relatives à l'«*échange transfrontière de justificatifs entre autorités compétentes*» visé à l'article 12, étant donné qu'elles sont les plus pertinentes pour la protection des données à caractère personnel. Ces recommandations sont discutées aux sections 3.1 à 3.5 ci-dessous et seront suivies d'une recommandation supplémentaire concernant d'autres éléments pertinents de la proposition dans les sections 3.6 et 3.7.

3.1. Base juridique de l'échange transfrontière de justificatifs (article 12)

L'article 12, paragraphe 1, dispose que pour certaines procédures en ligne spécifiques, un système technique pour l'échange électronique de justificatifs entre autorités compétentes de différents États membres est mis en place par la Commission (en coopération avec les États membres). La même disposition précise les procédures en ligne couvertes par le champ d'application de l'obligation d'utiliser ce système technique pour l'échange transfrontière de justificatifs.

En particulier, l'article 12, paragraphe 1, fait référence aux procédures prévues par les quatre directives suivantes: la directive sur la reconnaissance des qualifications professionnelles[45], la directive «services»[46], la directive sur les marchés publics[47] et la directive relative à la passation

de marchés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux[48].

L'article 12, paragraphe 1, fait également référence aux procédures en ligne énumérées à l'annexe II de la proposition. Il s'agit notamment des procédures suivantes:

- demande d'un certificat de naissance;
- demande d'une bourse d'études;
- enregistrement pour l'obtention des prestations de sécurité sociale;
- demande de reconnaissance de diplômes;
- changement d'adresse, demande ou renouvellement d'une carte d'identité ou d'un passeport, immatriculation d'un véhicule;
- demande d'une pension ou de prestations de préretraite;
- enregistrement général de l'activité économique; enregistrement d'un employeur (personne physique) auprès d'un organisme public ou semi-public de pension et d'assurance; enregistrement de salariés auprès d'un organisme public ou semi-public de pension et d'assurance;
- notification de la fin du contrat de travail d'un salarié aux régimes de sécurité sociale, paiement des cotisations sociales pour les salariés.

L'une des préoccupations majeures du CEPD est le fait que la base juridique du traitement des données à caractère personnel aux fins de l'échange transfrontière de justificatifs ne ressort pas suffisamment clairement de la proposition, en particulier, lorsque l'échange de justificatifs découle d'une obligation légale[49] ou de l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique[50].

En précisant que les autorités compétentes «*sollicitent le justificatif nécessaire directement auprès de l'autorité compétente de délivrance dans l'autre État membre par l'intermédiaire du système technique*» et que «*l'autorité de délivrance met le justificatif à disposition par l'intermédiaire dudit système*», l'article 12, paragraphe 4, semble suggérer que les autorités compétentes sont assujetties à une obligation légale de mettre le justificatif à disposition dès qu'il leur est demandé par leurs homologues de l'État membre demandeur. Ceci laisse à penser que la base juridique est soit une obligation légale, soit l'exécution d'une mission d'intérêt public. Le considérant 28, qui dispose que «*le présent règlement devrait [...] jeter les bases de l'échange direct de justificatifs entre les autorités compétences concernées [...] lorsque les citoyens ou les entreprises en font la demande*», semble également étayer cette dernière conclusion[51].

Pour garantir la sécurité juridique, le CEPD recommande de mentionner expressément la base juridique de l'échange de justificatifs dans une disposition de fond.

Avant de formuler une recommandation sur le choix à opérer entre ces options, il importe de distinguer la base juridique de l'échange de justificatifs proprement dit, d'une part, et la base juridique de l'échange de justificatifs par l'intermédiaire du système technique visé à l'article 12.

Comme indiqué au début de la présente section 3, s'agissant de l'échange de justificatifs proprement dit, l'article 12, paragraphe 1, fait référence à des procédures prévues dans les quatre directives qu'il énumère. De plus, l'article 12, paragraphe 1, fait également référence

aux procédures en ligne énumérées à l'annexe II de la proposition (sans préciser plus avant la base juridique de ces échanges).

Une autre question distincte est celle de savoir quelle est la base juridique retenue pour l'utilisation du système technique visé à l'article 12 pour l'échange de justificatifs.

Afin de contribuer à garantir la sécurité juridique, le CEPD recommande qu'un considérant soit ajouté afin de préciser que:

- la proposition elle-même ne prévoit pas de base juridique pour l'échange de justificatifs et que tout échange au titre de l'article 12, paragraphe 1, doit avoir une base juridique appropriée par ailleurs, telle que celle visée dans les quatre directives énumérées dans cette disposition ou dans le droit national ou de l'UE applicable;
- la base juridique de l'utilisation du système technique prévu à l'article 12 pour l'échange de justificatifs est l'exécution d'une mission d'intérêt public au sens de l'article 6, paragraphe 1, point a), du RGPD; et que
- les utilisateurs ont le droit de s'opposer au traitement de données à caractère personnel les concernant dans le système technique, en application de l'article 21, paragraphe 1, du RGPD.

3.2. Limitation de la finalité (article 12, paragraphe 6)

L'article 12, paragraphe 6, de la proposition limite «*uniquement [au] justificatif demandé*» l'échange transfrontière de justificatifs entre autorités compétentes pour les procédures en ligne.

Le CEPD se réjouit de l'intention de la Commission de respecter le principe de la limitation de la finalité. Comme indiqué à la section 2 ci-dessus, il s'agit d'un principe essentiel de la protection des données, qui impose que les données à caractère personnel soient «*collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités*»[52].

Ainsi que cela a été dit au début de cette section 3, conformément à l'article 12, paragraphe 1, de la proposition, le principe «une fois pour toutes» s'appliquerait à l'échange de justificatifs dans le cadre des procédures en ligne énumérées à l'annexe II. Il s'appliquerait, en outre, également à tout échange transfrontière de justificatifs au titre des quatre directives visées à l'article 12, paragraphe 1, de la proposition.

Comme expliqué à la section 2, le principe «une fois pour toutes» s'oppose potentiellement à celui de la limitation de la finalité en ce sens que des données à caractère personnel qui ont été collectées par des autorités publiques pour une finalité particulière ne devraient pas être redemandées, mais au contraire être traitées à des fins administratives futures. Cependant, le CEPD comprend que l'objectif de la proposition n'est pas d'autoriser un échange d'informations allant au-delà de ce qui est déjà prévu dans la législation sectorielle applicable de l'UE (à savoir les quatre directives susvisées) ou dans le droit de l'Union ou le droit national applicable. Il comprend également que la proposition ne tend pas à restreindre le principe de la limitation de la finalité énoncé à l'article 6, paragraphe 4, et à l'article 23, paragraphe 1, du RGPD.

Cependant, pour garantir la sécurité juridique, le CEPD recommande d'ajouter un considérant à la proposition afin de confirmer cette interprétation. Ce considérant devrait en particulier:

- préciser que la proposition ne contient pas de base juridique pour l'utilisation du système technique en vue d'échanger des informations pour des finalités autres que celles prévues dans les quatre directives énumérées ou prévues par ailleurs dans le droit de l'UE ou dans le droit national applicable;
- et que la proposition ne tend en aucune façon à restreindre le principe de la limitation de la finalité énoncé à l'article 6, paragraphe 4, et à l'article 23, paragraphe 1, du RGPD.

3.3. «Demande expresse de l'utilisateur» (article 12, paragraphe 4)

Comme expliqué à la section 1 ci-dessus, le CEPD se félicite des efforts déployés dans la proposition pour assurer la transparence et faire en sorte que les personnes physiques conservent le contrôle des données à caractère personnel les concernant, en exigeant «*une demande expresse de l'utilisateur*» avant tout transfert de justificatifs entre des autorités compétentes (article 12, paragraphe 4).

Afin d'améliorer encore le texte, le CEPD recommande que la proposition clarifie (dans des dispositions de fond et/ou dans des considérants, le cas échéant):

- ce qu'est une demande «*expresse*» et dans quelle mesure la demande doit être spécifique;
- si la demande peut être introduite par l'intermédiaire du système technique visé à l'article 12, paragraphe 1;
- quelles sont les conséquences si l'utilisateur choisit de ne pas formuler de «*demande expresse*» *et*
- si une telle demande peut être retirée.

Ces précisions peuvent contribuer à ce que le système technique soit conçu de telle sorte qu'il donne un niveau de contrôle adéquat aux personnes utilisant le système, tout en assurant un flux efficace d'informations.

Le CEPD recommande en particulier que:

- un considérant précise qu'une demande ne peut être considérée comme *expresse* que si elle contient une indication libre, spécifique, informée et univoque du souhait de la personne concernée que les informations pertinentes soient échangées, soit dans une déclaration, soit par une action positive;
- le même considérant précise également qu'une demande expresse d'échange de justificatifs ne peut pas simplement être déduite d'une demande de réaliser une procédure administrative particulière (par exemple, immatriculer un véhicule); il n'est pas suffisant non plus de formuler une demande générale, comme demander tous les documents nécessaires auprès de toutes les autorités compétentes aux fins de la procédure administrative en cause;
- l'article 12, paragraphe 2, qui énumère les exigences auxquelles le système technique doit répondre, inclut un alinéa supplémentaire spécifique en vertu duquel le système « *permettra le traitement de la demande expresse de l'utilisateur visée au paragraphe 4 ainsi que le retrait de celle-ci* »;

- une disposition de fond clarifie qu'alors que l'utilisation du système technique est recommandée non seulement pour les autorités qui échangent des justificatifs mais aussi pour les utilisateurs qui interagissent avec ces autorités (en particulier, pour introduire une demande et visualiser le justificatif avant l'échange), un utilisateur peut aussi introduire une demande en dehors du système technique (en d'autres termes, les utilisateurs ne sont pas tenus de passer par le système technique pour introduire une demande: ils peuvent l'introduire directement par d'autres moyens en dehors du système technique);
- une disposition de fond ou un considérant précisent qu'aucun échange de justificatifs ne peut passer par le système technique si l'utilisateur n'a pas fait de demande expresse ou l'a retirée;
- une disposition de fond précise si l'utilisateur peut ou non également présenter le justificatif sans recourir au système technique (en d'autres termes, si les utilisateurs sont tenus de recourir au système technique pour la présentation de justificatifs);
- l'article 12, paragraphe 4, précise que l'utilisateur peut retirer sa demande d'échange de justificatifs à tout moment; un considérant peut alors indiquer qu'un utilisateur peut choisir de retirer sa demande en motivant ou non son retrait, mais, en règle générale, un retrait peut avoir lieu lorsque, par exemple, après la «*prévisualisation*» des justificatifs au titre de l'article 12, paragraphe 2, point e), il découvre que l'information est inexacte, obsolète ou va au-delà de ce qui est nécessaire aux fins de la procédure en cause (par exemple, un document énumère toutes les adresses antérieures enregistrées au cours des cinq dernières années plutôt que simplement l'adresse actuelle, qui est la seule pertinente aux fins de la procédure en cause).

3.4. «*Visualisation du justificatif avant l'échange*» (article 12, paragraphe 2, point e))

Ainsi que cela a également été expliqué à la section 1 ci-dessus, outre l'exigence d'un consentement explicite, offrir à l'utilisateur la possibilité de «*visualiser le justificatif avant l'échange*» (article 12, paragraphe 2, point e)) peut également contribuer grandement à la transparence et au contrôle par l'utilisateur. Surtout, cette possibilité peut également contribuer à faire en sorte que tout justificatif échangé soit adéquat, pertinent, limité à ce qui est nécessaire par rapport aux finalités pour lesquelles les données sont traitées («*minimisation des données*»), exact et, si nécessaire, actualisé («*exactitude*»).

Pour améliorer davantage le texte, le CEPD recommande que:

- la proposition précise quels sont les choix qui s'offrent à l'utilisateur qui met à profit la possibilité de «*visualiser*» les données avant l'échange;
- en particulier, l'article 12, paragraphe 2, point e), devrait clarifier que l'utilisateur a la possibilité de visualiser le justificatif en temps utile avant qu'il ne soit accessible au destinataire et qu'il peut retirer la demande d'échange du justificatif (voir également les recommandations connexes sur les «*demandes expresses*»);
- ceci peut se faire, par exemple, en insérant le segment qui suit à la fin de l'article 12, paragraphe 2, point e): «*avant qu'il soit accessible à l'autorité demandeuse et de retirer sa demande à tout moment* ».

De plus, pour rappeler aux organisations pertinentes leurs obligations au titre du RGPD en matière de transparence, le CEPD souligne que les organisations qui échangent des justificatifs par le biais du système technique doivent également veiller à ce que les utilisateurs reçoivent des informations claires sur la manière dont les données à caractère personnel les concernant

seront traitées. Cette obligation est imposée aux responsables du traitement par les articles 13 et 14 du RGPD et par les articles 11 et 12 du règlement n° 45/2011. Le CEPD recommande donc d'inclure une référence à ces exigences dans un considérant.

Enfin, le CEPD souligne que, si le mécanisme de visualisation avant l'échange peut contribuer à garantir le respect des exigences en matière de qualité des données, il découle des règles généralement applicables à la protection des données que les autorités devraient néanmoins mettre en place des procédures efficaces pour s'assurer que les données à caractère personnel sont mises à jour si nécessaire et que les données inexactes ou obsolètes ne sont plus traitées[53].

3.5. Définition d'un justificatif, éventail des procédures en ligne couvertes (article 3, paragraphe 4, et article 2, paragraphe 2, point b))

L'article 3, paragraphe 4, de la proposition définit le terme «*justificatif*» comme étant «*tout document ou toutes données, y compris du texte ou des enregistrements sonores, visuels ou audiovisuels, sur tout support, qui sont émis par une autorité compétente en vue d'attester la véracité de faits ou le respect d'exigences dans le contexte de procédures mentionnées à l'article 2, paragraphe 2, point b)*».

La définition est large et peut potentiellement inclure un large éventail de données à caractère personnel. Il apparaît également que la définition couvre non seulement des documents disponibles, mais également tout extrait de ces documents ou d'autres informations ou données disponibles auprès de l'autorité compétente sollicitée dans n'importe quel format.

L'éventail de données à caractère personnel qui peuvent potentiellement être échangées est toutefois limité par la référence à l'article 2, paragraphe 2, point b), de la proposition, laquelle renvoie à l'article 2, paragraphe 2, point a), et à l'annexe I. Cette annexe dresse une longue liste de secteurs, allant des voyages, du travail et de la retraite à l'intérieur de l'Union aux marchés publics ou à l'exploitation d'une entreprise en passant par les soins de santé. Surtout, la liste de l'annexe I n'est pas identique et semble nettement plus large et plus générale que la portée autorisée de l'échange transfrontière de justificatifs au titre de l'article 12, paragraphe 1, qui fait référence à l'annexe II (beaucoup plus courte et spécifique) ainsi qu'à quatre directives spécifiquement visées.

Le CEPD recommande que les deux dispositions soient alignées afin de garantir la cohérence et la sécurité juridique. De manière générale, du point de vue de la protection des données à caractère personnel, plus la portée de tout échange d'informations est clairement définie, plus la sécurité juridique est grande et plus le risque d'échanges de justificatifs contraires à la législation en matière de protection des données est réduit.

En principe, le CEPD recommanderait donc:

- de clarifier le lien entre l'article 2, paragraphe 2, point b), et l'article 3, paragraphe 4, d'une part, et l'article 12, paragraphe 1, d'autre part;
- le CEPD souligne également qu'il se félicite des efforts déployés par la Commission dans la proposition en vue de limiter l'échange d'informations aux procédures en ligne énumérées à l'annexe II et dans les quatre directives spécifiquement visées;
- il recommande donc que le champ d'application de la proposition reste clairement défini et continue d'inclure l'annexe II et les références aux quatre directives spécifiquement visées.

3.6. Autres recommandations: modifications du règlement IMI (article 36)

Utilisation possible de l'IMI pour la coopération au sein du comité européen de la protection des données

L'article 36, paragraphe 1, de la proposition garantit que les participants IMI (tels que définis dans le règlement IMI) englobent désormais non seulement les autorités compétentes des États membres et la Commission, mais aussi des organes et organismes de l'Union. Ce changement permettrait potentiellement au CEPD et au comité européen de la protection des données d'utiliser le système IMI pour échanger des informations dans le cadre du RGPD.

Une coopération transfrontière entre les autorités de contrôle nationales chargées de la protection des données, le CEPD, le comité européen de la protection des données et la Commission est nécessaire pour mettre en œuvre le RGPD de telle sorte qu'il puisse atteindre ses deux objectifs: la protection des libertés et droits fondamentaux des personnes à l'égard du traitement de données à caractère personnel, d'une part, et la libre circulation de ces données au sein de l'Union, d'autre part. La libre circulation des données au sein de l'Union est une condition préalable au fonctionnement du marché intérieur.

Le RGPD renforce les mécanismes permettant une application plus harmonieuse de la protection des données et introduit de nouveaux modes de coopération entre autorités nationales à cet effet. Il prévoit que les autorités utilisent des moyens électroniques d'échange d'informations. Dans la mesure où le système d'information du marché intérieur (IMI) est conçu pour permettre d'échanger efficacement des informations entre les participants IMI, il devrait être mis à disposition afin de renforcer la coopération dans le domaine de la protection des données, lorsque les autorités le jugent approprié.

Par conséquent, le CEPD:

- se félicite de l'inclusion des organes de l'UE dans la définition des acteurs de l'IMI dans la proposition et
- recommande en outre d'ajouter le RGPD à l'annexe du règlement IMI afin de permettre l'utilisation potentielle de l'IMI aux fins de la protection des données.

Le CEPD souhaite également clarifier que la recommandation d'inclure le RGPD dans l'annexe du règlement IMI s'applique, indépendamment du fait que le législateur décide ou non d'inclure la protection des données dans le champ d'application du portail numérique unique («SGD»). Même en cas d'indisponibilité du SDG dans ce domaine, la coopération entre les autorités de contrôle nationales chargées de la protection des données, le CEPD, le comité européen de la protection des données et la Commission peut tirer profit d'un accès à l'IMI.

Surveillance coordonnée par le CEPD et les autorités de contrôle nationales chargées de la protection des données

Comme cela a déjà été souligné à la section 1, le CEPD se félicite de la modification proposée au règlement IMI, qui confirme et actualise les dispositions relatives au mécanisme de surveillance coordonnée de l'IMI afin de garantir une approche cohérente (article 36, paragraphe 6, point b)).

Cette modification prévoit que les autorités de contrôle nationales (chargées de la protection des données), «*agissant chacun[e] dans les limites de leurs compétences respectives, coopèrent en vue d'assurer une surveillance coordonnée de l'IMI et de son utilisation par les participants IMI conformément à l'article 62 du [règlement (UE) XX/201Y]*».

Cette référence renvoie au règlement proposé qui remplacera le règlement n° 45/2011 et offre un modèle unique cohérent pour la surveillance coordonnée[54].

Comme il l'a déjà indiqué dans son avis 5/2017 sur le renforcement des règles de protection des données pour les institutions et organes de l'UE[55], le CEPD se réjouit de l'approche consistant à mettre en place un modèle de contrôle coordonné, unique et cohérent pour les systèmes d'information à grande échelle de l'UE, dans la mesure où cela permettra de renforcer l'intégrité, l'efficacité et la cohérence du contrôle en matière de protection des données et de garantir un environnement harmonieux en vue du développement de la protection des données dans les années à venir.

Le CEPD croit comprendre que le but est d'utiliser ce modèle pour contrôler tant les futurs systèmes que les systèmes existants. Il constate que le considérant 65 de la proposition[56] prévoit spécifiquement que «*[l]e cas échéant, la Commission devrait donc soumettre des propositions législatives visant à amender les actes législatifs de l'Union prévoyant un modèle de contrôle coordonné, afin de les aligner sur le modèle de contrôle coordonné prévu par le présent règlement*». Le CEPD se réjouit d'une telle simplification du règlement IMI dans le cadre de l'article 36, paragraphe 6, point b), de la proposition actuelle.

3.7. La protection des données en tant que domaine d'information et les autorités chargées de la protection des données en tant que mécanismes de résolution de problèmes (article 2 et annexes I et III)

L'article 2, paragraphe 2, point a), de la proposition dispose que le portail numérique unique donne accès à des informations sur les droits, les obligations et les règles dans les domaines énumérés à l'annexe I (par exemple, les voyages dans l'Union, le séjour dans un autre État membre, le démarrage, la gestion d'une entreprise et la cessation d'activité). Ces domaines sont pertinents pour les personnes physiques et les entreprises souhaitant exercer leurs droits dérivés du droit de l'Union dans le domaine du marché intérieur.

Compte tenu de l'importance des flux transfrontières de données à caractère personnel pour le fonctionnement du marché intérieur, le CEPD recommande d'ajouter la protection des données à caractère personnel aux domaines d'information de l'annexe I.

L'article 2, paragraphe 2, point c), de la proposition dispose que le portail numérique unique donne accès à des informations sur des services d'assistance et de résolution de problèmes ainsi qu'à des liens y renvoyant. Ces services sont énumérés à l'annexe III (par exemple, guichets uniques, EURES, règlement en ligne des litiges). L'une des tâches des autorités de contrôle chargées de la protection des données étant d'informer les personnes concernées de leurs droits au titre du RGPD et de traiter les plaintes introduites par les personnes concernées, le CEPD recommande d'ajouter les autorités de contrôle chargées de la protection des données à la liste des services d'assistance et de résolution de problèmes énumérés à l'annexe III.

4. CONCLUSIONS

Le CEPD se félicite de la proposition de la Commission de moderniser les services administratifs en améliorant la disponibilité, la qualité et l'accessibilité des informations au sein de l'Union européenne et apprécie la consultation et les préoccupations de la Commission et du Parlement quant à l'impact que cette proposition pourrait avoir sur la protection des données à caractère personnel.

En plus de formuler des recommandations spécifiques visant à poursuivre l'amélioration qualitative de la législation, le CEPD tient également à saisir cette occasion de donner un premier aperçu des questions clés liées au principe «une fois pour toutes» en général, bien qu'un grand nombre d'entre elles ne découlent pas nécessairement de la proposition sous sa forme actuelle. Ces questions portent notamment sur:

- la base juridique du traitement,
- la limitation de la finalité
- et les droits des personnes concernées.

Le CEPD insiste sur le fait que pour assurer une mise en œuvre réussie du principe «une fois pour toutes» et permettre un échange transfrontière licite des données, ledit principe doit être appliqué conformément aux principes pertinents de la protection des données.

S'agissant de la proposition proprement dite, le CEPD soutient:

- les efforts déployés pour s'assurer que les personnes gardent le contrôle des données à caractère personnel les concernant, notamment en exigeant «*une demande expresse de l'utilisateur*» avant tout transfert de justificatifs entre autorités compétentes (article 12, paragraphes 2 et 4) et en offrant à l'utilisateur la possibilité de «*visualiser le justificatif avant l'échange*» (article 12, paragraphe 2, point e));
- les efforts déployés pour définir le champ d'application matériel du principe «une fois pour toutes» (article 12, paragraphe 1) et
- il se félicite en outre de la modification proposée au règlement IMI, qui confirme et actualise les dispositions relatives au mécanisme de surveillance coordonnée de l'IMI en vue d'assurer une approche cohérente (article 36, paragraphe 6, point b));
- il se réjouit également de l'inclusion des organes de l'UE dans la définition des participants IMI dans la proposition, ce qui peut contribuer à aider le comité européen de la protection des données à exploiter les possibilités techniques offertes par l'IMI pour l'échange d'informations.

S'agissant de la base juridique du traitement, le CEPD recommande qu'un ou plusieurs considérants soient ajoutés pour préciser que:

- la proposition proprement dite ne prévoit pas de base juridique pour l'échange de justificatifs et que tout échange au titre de l'article 12, paragraphe 1, doit avoir une base juridique appropriée par ailleurs, comme dans les quatre directives énumérées dans cette disposition ou dans le droit l'Union ou dans le droit national applicable;
- la base juridique pour l'utilisation du système technique prévu à l'article 12 pour l'échange de justificatifs est l'exécution d'une mission d'intérêt public au sens de l'article 6, paragraphe 1, point a), du RGPD; et que

- les utilisateurs ont le droit de s'opposer au traitement de données à caractère personnel les concernant dans le système technique, en application de l'article 21, paragraphe 1, du RGPD.

S'agissant de la limitation de la finalité, le CEPD recommande qu'un ou plusieurs considérants soient ajoutés pour préciser que:

- la proposition ne contient pas de base juridique pour l'utilisation du système technique en vue d'échanger des informations pour des finalités autres que celles visées dans les quatre directives énumérées ou prévues par ailleurs dans le droit de l'Union ou dans le droit national applicable;
- et que la proposition ne tend en aucune façon à restreindre le principe de la limitation de la finalité énoncé à l'article 6, paragraphe 4, et à l'article 23, paragraphe 1, du RGPD.

S'agissant de la notion de «*demande expresse*», le CEPD recommande que la proposition clarifie (de préférence, dans une disposition de fond):

- ce qu'est une demande «*expresse*» et dans quelle mesure la demande doit être spécifique;
- si la demande peut être soumise par l'intermédiaire du système technique visé à l'article 12, paragraphe 1;
- quelles sont les conséquences si l'utilisateur choisit de ne pas formuler de «*demande expresse*» et
  si une telle demande peut être retirée. (Pour les recommandations spécifiques, voir la section 3.3 ci-dessus.)

S'agissant de la question de la «*visualisation avant l'échange*», le CEPD recommande que:
- la proposition précise quels sont les choix qui s'offrent à l'utilisateur qui met à profit la possibilité de «*visualiser*» les données avant l'échange;
- en particulier, l'article 12, paragraphe 2, point e), devrait clarifier que l'utilisateur a la possibilité de visualiser le justificatif en temps utile avant qu'il ne soit accessible au destinataire et qu'il peut retirer la demande d'échange du justificatif (voir également les recommandations connexes sur les «*demandes expresses*»);
- ceci peut se faire, par exemple, en insérant le segment suivant à la fin de l'article 12, paragraphe 2, point e): «*avant qu'il soit accessible à l'autorité demandeuse et de retirer sa demande à tout moment* ».

S'agissant de la définition d'un justificatif et de l'éventail de procédures en ligne couvertes, le CEPD recommande:

- de remplacer la référence à l'article 2, paragraphe 2, point b), à l'article 3, paragraphe 4, par une référence à l'article 12, paragraphe 1, ou de proposer une autre solution législative produisant un effet similaire;
- le CEPD souligne également qu'il se félicite des efforts déployés par la Commission dans la proposition en vue de limiter l'échange d'informations aux procédures en ligne énumérées à l'annexe II et dans les quatre directives spécifiquement visées;
- il recommande donc que le champ d'application de la proposition reste clairement défini et continue d'inclure l'annexe II et les références aux quatre directives spécifiquement visées.

Enfin, le CEPD recommande:

- d'ajouter le RGPD à l'annexe du règlement IMI afin de permettre l'utilisation potentielle de l'IMI aux fins de la protection des données; et
- d'ajouter les autorités de contrôle de la protection des données à la liste des services d'assistance et de résolution de problèmes énumérés à l'annexe III.

Bruxelles, le 1er août 2017

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

Notes

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 119 du 4.5.2016, p. 1.
[3] JO L 8 du 12.1.2001, p. 1.
[4] Proposition de règlement du Parlement européen et du Conseil établissant un programme numérique unique pour donner accès à des informations, des procédures et des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) nº 1024/2012, COM(2017) 256 final, 2017/0086 (COD) (ci-après «la proposition»).
[5] Exposé des motifs de la proposition, p. 2.
[6] Règlement (UE) nº 1024/2012 du Parlement européen et du Conseil du 25 octobre 2012 concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur et abrogeant la décision 2008/49/CE de la Commission («*règlement IMI*»), JO L 316 du 14.11.2012, p. 1.
[7] Voir aussi l'avis du CEPD du 22 novembre 2011 sur la proposition de la Commission de règlement du Parlement européen et du Conseil concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur
(«*IMI*») disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/11-11-22_imi_opinion_fr.pdf
[8] Voir aussi article 14 de la proposition de directive du Parlement européen et du Conseil relative au cadre juridique et opérationnel applicable à la carte électronique européenne de services introduite par le règlement ... [Règlement CES], (COM (2016) 823 final, 2016/0402(COD).
[9] Considérant 28 de la proposition.
[10] Article 12, paragraphes 1 et 4, de la proposition.
[11] À titre d'exemple, dans leur premier document de prise de position, les partenaires du projet relatif au principe «une fois pour toutes» reconnaissent que les États membres interprètent ce principe différemment: certains considèrent qu'il concerne le stockage des données, par lequel la législation nationale impose aux autorités de stocker les données dans une seule base de données, tandis que d'autres considèrent qu'il se rapporte à la collecte des données et autorise le stockage de données dans plusieurs entrepôts. Krimmer et al, «Position paper on definition of OOP and situation in Europe», p. 9, disponible à l'adresse http://toop.eu/sites/default/files/D2.6_Position%20paper%20on%20definition%20of%20OOP%20and%20situation%20in%20Europe.pdf. Voir aussi l'étude Smart, précitée, p. 7. Voir aussi la discussion sur les «sources faisant autorité» et les «référentiels» (van Alsenoy et al., p. 256 et 257, et annexe IX de l'«étude Smart», p. 192 et seq.).
[12] Commission européenne, «Plan d'action européen 2016-2020 pour l'administration en ligne», COM(2016) 179 final, p. 2.
[13] «EU-wide digital Once-Only Principle for citizens and businesses», étude préparée pour la DG Réseaux, contenu & technologie de la Commission européenne, SMART 2015/0062 («étude Smart»), disponible à l'adresse: https://ec.europa.eu/digital-single-market/en/news/eu-wide-digital-once-only-principle-citizens-and-businesses-policy-options-and-their-impacts. Voir aussi le document d'orientation estonien sur la libre circulation des données - la cinquième liberté de l'Union européenne, p. 18 et 19, disponible à l'adresse https://www.eu2017.ee/news/insights/FreeMovementOfData
[14] Étude Smart, précitée.
[15] Plan d'action européen 2016-2020 pour l'administration en ligne, précité, p. 3.
[16] Étude Smart, précitée, p. 4.
[17] Plan d'action européen 2016-2020 pour l'administration en ligne, précité, p. 3.
[18] Étude Smart, précitée, p. 45.
[19] Voir aussi le document d'orientation estonien sur la libre circulation des données - la cinquième liberté de l'Union européenne, p. 18, disponible à l'adresse: https://www.eu2017.ee/news/insights/FreeMovementOfData
[20] Précité.
[21] Article 6, paragraphe 1, point a), du RGPD.
[22] Article 6, paragraphe 1, point c), du RGPD.
[23] Article 6, paragraphe 1, point e), du RGPD.
[24] Voir aussi l'étude Smart, précitée, p. 17, 19 et 46 à 48.
[25] Avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement, adopté le 13 juillet 2011 (WP 187), disponible à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf.
[26] Article 4, paragraphe 11, article 7, considérants 32, 42 et 43 du RGPD.
[27] Considérant 43 du RGPD. Voir également avis 15/2011 du groupe de travail «Article 29».
[28] Article 6, paragraphe 1, point c).

[29] Avis 6/2014 du groupe de travail «Article 29» sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, adopté le 9 avril 2014 (WP 217), p. 19, disponible à l'adresse: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf
[30] Précité.
[31] Précité, p. 19.
[32] Précité.
[33] Considérant 45 du RGPD.
[34] Précité, p. 21.
[35] Article 21, paragraphe 1, du RGPD.
[36] Voir aussi avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité, adopté le 2 avril 2013 (WP 203), disponible à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (en anglais)
[37] Voir article 6, paragraphe 4, du RGPD. Pour être complet, voir aussi l'article 5, paragraphe 1, point b), qui dispose que le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales. Cette exception spécifique, tout en étant potentiellement pertinente dans certains cas de partage de données entre autorités publiques, n'est pas directement pertinente aux fins du principe «une fois pour toutes» et ne sera donc pas discutée plus avant dans le présent avis.
[38] Avis 7/2015 du CEPD: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_fr.pdf. Voir en particulier la section 3.
[39] Avis 9/2016 du CEPD du 20 octobre 2016 sur les systèmes de gestion des informations personnelles, JO 463 du 13.12.2016, p. 10, disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_fr.pdf.
Voir, notamment, les paragraphes 36, 50 et 57.
[40] La transparence est une condition préalable à un exercice effectif des droits relatifs à la protection des données et elle est importante dans l'instauration de la confiance. Voir, par exemple, le document d'orientation estonien sur la libre circulation des données – la cinquième liberté de l'Union européenne, p. 19, disponible à l'adresse: https://www.eu2017.ee/news/insights/FreeMovementOfData. Voir aussi l'arrêt dans l'affaire C-201/14, *Smaranda Bara e.a./Casa Naţională de Asigurări de Sănătate e.a.*, EU:C:2015:638.
[41] Article 5 du RGPD.
[42] Article 25 du RGPD.
[43] Article 5, paragraphe 2, du RGPD.
[44] Étude Smart, précitée, p. 211.
[45] Directive 2005/36/CE du Parlement européen et du Conseil européen du 7 décembre 2005 relative à la reconnaissance des qualifications professionnelles (JO L 30 du 30.9.2005, p. 22-142).
[46] Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur (JO L 376 du 27.12.2006, p. 36-68).
[47] Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65-242).
[48] Directive 2014/25/UE du Parlement européen et du Conseil du 26 février 2014 relative à la passation de marchés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux (JO L 94 du 28.3.2014, p. 243-374).
[49] Article 6, paragraphe 1, point c), du RGPD.
[50] Article 6, paragraphe 1, point e), du RGPD.
[51] Voir aussi l'étude Smart, p. 24 à 26.
[52] Article 5, paragraphe 1, point b), du RGPD.
[53] Voir aussi l'étude Smart, précitée, p. 52.
[54] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE.
[55] Avis 5/2017 du CEPD sur le renforcement des règles de protection des données pour les institutions et organes de l'UE (sous-titre: Avis du CEPD sur la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/17-03-15_regulation_45-2001_fr.pdf, paragraphes 77 et 78.
[56] Précité.