



**1806/16/FR
WP 239**

**Avis 2/2016 sur la publication de données à caractère personnel aux fins de la
transparence dans le secteur public**

Adopté le 8 juin 2016

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale Justice et consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/index_en.htm

1. INTRODUCTION

1.1 CHAMP D'APPLICATION DE L'AVIS

Le présent avis explique comment appliquer les principes de la protection des données au traitement et à la publication de données à caractère personnel aux fins de la transparence dans le secteur public, notamment dans le cadre des mesures anticorruption ainsi que de la gestion et de la prévention des conflits d'intérêts¹. Il n'a pas vocation à déterminer quelles devraient être les informations disponibles au titre de la législation des États membres de l'Union en matière d'accès aux documents publics ou de liberté d'information², ne restreint pas la disponibilité de ces informations publiques telle que prévue par le droit national et ne porte pas non plus sur la mise en œuvre des règlements (CE) n^{os} 45/2001 et 1049/2001³ applicables aux institutions et organes de l'Union.

D'une manière générale, les organismes du secteur public peuvent être tenus de collecter, d'enregistrer et de conserver des informations sur leurs activités et leur personnel, et de les mettre à la disposition du public, le plus souvent sur leur site internet officiel. Ce type de traitement est susceptible d'impliquer le traitement de données à caractère personnel, y compris leur diffusion auprès du public.

Le présent avis s'adresse aux autorités législatives nationales, aux gouvernements, services ou organismes nationaux et aux autres institutions compétentes (ci-après les «institutions compétentes») du secteur public chargées de la lutte contre la corruption, de la prévention des conflits d'intérêts et d'autres obligations de transparence, ainsi qu'aux autorités de protection des données. Il propose des recommandations sur la base d'une interprétation commune du cadre de protection des données dans lequel de tels traitements sont effectués. Il traite notamment de la mise en œuvre générale des principes et des valeurs de la directive 95/46/CE⁴ et du règlement général sur la protection des données (ci-après le «règlement général»).

¹ Aux fins du présent avis, on entend par «secteur public» l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public, sans préjudice des définitions inscrites dans le droit des États membres.

² Pour plus de détails, voir l'avis 6/2013 du GT 29 sur la réutilisation des informations du secteur public (ISP) et des données ouvertes.

³ Règlement (CE) n° 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, et règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission.

⁴ 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.

Les articles 1^{er} et 4 de la directive 95/46/CE disposent que les États membres doivent assurer la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel. Les États membres doivent également veiller à ce que les traitements de données à caractère personnel effectués dans le cadre des mesures anticorruption visant à gérer les conflits d'intérêts potentiels et les obligations de transparence y afférentes soient réglementés par les dispositions nationales qu'ils adoptent en application de cette directive et à la lumière du règlement général.

1.2 OBJECTIF DE L'AVIS

Le présent avis a pour but de fournir aux législateurs des États membres et aux institutions compétentes des orientations pratiques, des recommandations et des exemples des meilleures pratiques concernant les moyens d'assurer le respect du droit à la protection des données tout en prenant en considération et en satisfaisant l'intérêt public légitime à la transparence lorsque les initiatives législatives et politiques sur ces questions exigent la diffusion d'informations concernant une personne physique. La notion de «transparence»⁵ est liée aux principes d'ouverture, de bonne administration et de bonne gouvernance consacrés dans les traités⁶ et dans la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»)⁷.

L'impartialité et la déontologie des agents publics, de même que la transparence de leur action, sont reconnues comme des valeurs essentielles pour garantir un niveau d'excellence et de qualité dans l'exercice des responsabilités publiques correspondantes. Il convient de trouver un équilibre entre, d'une part, les droits des agents publics à la protection de leurs données⁸ et, d'autre part, l'intérêt public à ce que ces personnes s'acquittent de leurs tâches et de leurs responsabilités d'une manière transparente. La publication d'informations sur les intérêts privés d'agents publics fait partie de l'éventail des mesures utilisées pour gérer les conflits d'intérêts potentiels, renforcer l'obligation de rendre des comptes et conforter la confiance du public. Alors que les législations et réglementations encadrant la gestion des conflits d'intérêts varient d'un pays à l'autre, le présent avis formule des conseils sur la manière de garantir aux agents publics de tous les États membres le même niveau de protection des données.

2. CADRE JURIDIQUE

Aux termes de l'article 7 de la charte, toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. En outre, selon l'article 8 de la charte,

⁵ Cette référence est sans préjudice des définitions spécifiques inscrites dans les législations et les politiques nationales; elle n'est donnée qu'à la seule fin de faciliter la compréhension du présent avis.

⁶ Voir articles 10 et 11 du traité sur l'Union européenne et articles 15 et 298 du traité sur le fonctionnement de l'Union européenne.

⁷ Voir article 41 de la charte.

⁸ Les droits à la protection des données s'entendent comme les droits protégés par la directive relative à la protection des données et le règlement général.

toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. De même, l'article 8 de la convention européenne des droits de l'homme (ci-après la «CEDH») dispose que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance, et qu'il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre ou à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

L'article 6 de la directive 95/46/CE pose les principes de base du traitement des données à caractère personnel, tandis que son article 7 énonce les principes relatifs à la légitimation des traitements de données. Les considérants du règlement général précisent que la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public laisse intact et n'affecte en rien le niveau de protection des personnes physiques à l'égard du traitement des données à caractère personnel garanti par les dispositions du droit de l'Union et du droit des États membres.

Selon l'article 10 de la CEDH, toute personne a droit à la liberté d'expression. La Cour européenne des droits de l'homme a reconnu à plusieurs reprises, dans des affaires qui ne concernaient pas uniquement les médias ou les journalistes professionnels, que ce droit comprend «le droit du public à être dûment informé» et «le droit de recevoir des informations»⁹.

À la lumière des dispositions précitées, il est recommandé que les principes ci-après soient pris en considération lors du traitement de données à caractère personnel dans le cadre de la lutte contre les conflits d'intérêts et des mesures de transparence qui lui sont associées.

3. PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

L'article 6 de la directive 95/46/CE dispose que les données à caractère personnel doivent être:

- traitées loyalement et licitement;

⁹ Toutefois, jusqu'à ces dernières années, la Cour européenne des droits de l'homme considérait que la liberté de recevoir des informations, telle que garantie par l'article 10, ne saurait se comprendre comme imposant à un État une obligation positive de diffusion ou de divulgation d'informations au public [voir affaires *Leander c. Suède* (1987), *Gaskin c. Royaume-Uni* (1989), *Guerra c. Italie* (1998) et *Sîrbu c. Moldavie* (2004)]. Ce n'est que dans deux affaires récentes qu'elle semble s'être acheminée vers une interprétation plus large de la notion de liberté d'information (voir décision de 2006 sur la recevabilité de la requête dans l'affaire *Sdružení Jihočeské Matky c. République tchèque*, et arrêt de 2009 dans l'affaire *Társaság a Szabadságjogokért c. Hongrie*).

- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;
- exactes et, si nécessaire, mises à jour;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.

Les exigences précitées sont reprises dans les dispositions équivalentes du règlement général.

3.1 TRAITEMENT LOYAL ET LICITE

La base juridique du traitement de données à caractère personnel dans le cadre des mesures de lutte contre les conflits d'intérêts réside dans l'article 7, point c), de la directive 95/46/CE¹⁰. Aux termes de cette disposition, un traitement de données à caractère personnel peut être effectué s'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. Le traitement doit alors être déterminé par la loi¹¹. Il importe d'éviter l'insertion de clauses générales, afin de ne pas laisser au responsable du traitement une marge de manœuvre excessive dans la façon de se conformer à l'obligation légale¹².

Dans ces conditions, il est du devoir des législateurs de veiller à ce que l'obligation légale assure un juste équilibre entre les différents intérêts en jeu. Il faut en effet que la loi soit compatible avec le droit au respect de la vie privée et familiale et à la protection des données à caractère personnel, conformément à l'article 8 de la CEDH et aux articles 7 et 8 de la

¹⁰ Pour une analyse plus détaillée, voir l'avis 06/2014 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 (WP 217). Dans certains pays, il pourrait être possible d'invoquer l'article 7, point f), comme base pour le traitement de ce type de données à caractère personnel.

¹¹ Dans son avis 06/2014, le GT 29 souligne que, pour que l'article 7, point c), puisse s'appliquer, l'obligation doit être imposée par la loi, laquelle doit remplir toutes les conditions requises pour rendre l'obligation valable et contraignante. Il indique à ce propos que «[l]a législation peut, dans certains cas, définir seulement un objectif général, tandis que des obligations plus spécifiques sont imposées à un niveau différent, par exemple, dans le droit dérivé ou dans une décision contraignante d'une autorité publique dans un cas concret». Le considérant 41 du règlement général précise, à cet égard, que «[l]orsque le [...] règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné». Voir aussi article 6, paragraphe 3, du règlement général.

¹² Ibid.

charte¹³. Cela signifie que l'obligation légale de traiter des données à caractère personnel doit être nécessaire et proportionnée au but légitime recherché aussi bien que conforme au principe de limitation de la finalité.

Les institutions pourraient également invoquer l'article 7, point e), de la directive 95/46/CE comme base pour le traitement de données à caractère personnel dans le cadre qui nous occupe. Pour apprécier si les opérations de traitement respectent l'article 7, point e), et compte tenu des différents intérêts en présence, les institutions doivent s'assurer des points suivants:

- l'activité de traitement est une mission d'intérêt public ou relevant de l'exercice de l'autorité publique¹⁴;
- l'opération de traitement est nécessaire à l'exécution de cette mission ou à l'exercice de cette autorité (en d'autres termes, de telles opérations doivent être aptes à réaliser l'objectif poursuivi et ne pas aller au-delà de ce qui est nécessaire pour l'atteindre).

EXEMPLE: L'indexation¹⁵ des données à caractère personnel fournies sur une plateforme de transparence, dans le but de permettre aux citoyens d'y effectuer des recherches, peut être considérée comme une opération nécessaire. L'indexation des données d'identité pour les besoins d'un moteur de recherche externe n'est, par défaut, pas considérée comme nécessaire pour réaliser l'objectif de transparence.

3.2 PRINCIPES DE PROPORTIONNALITÉ, DE MINIMISATION ET DE QUALITÉ DES DONNÉES

Pour mettre en œuvre ces principes, il est tout d'abord nécessaire de déterminer les principaux objectifs du traitement de données. Par exemple, des initiatives de transparence peuvent avoir pour finalité de favoriser la diffusion de connaissances sur les décisions et les actions du gouvernement et de ses organes administratifs, en apportant un éclairage fondamental sur leurs processus, leurs opérations et leur personnel. Cela permet au public de demander compte aux gouvernements de la manière dont ils exécutent leurs missions et gèrent les ressources publiques, et de promouvoir ainsi la performance et l'efficacité. Les mesures considérées dans le présent avis visent à prévenir, détecter et sanctionner les conflits d'intérêts, dans le souci d'empêcher que des intérêts privés n'influent sur l'exercice de responsabilités publiques, d'améliorer l'intégrité, l'objectivité et l'impartialité des agents du secteur public, et de renforcer la confiance des citoyens dans leur gouvernement.

¹³ Voir arrêts de la Cour de justice de l'Union européenne du 20 mai 2003, Österreichischer Rundfunk, affaires jointes C-465/00, C-138/01 et C-139/01, et du 9 novembre 2010, Volker und Markus Schecke, affaires jointes C-92/09 et C-93/09.

¹⁴ Comme le souligne le GT 29 dans son avis 06/2014, la mission d'intérêt public ou l'autorité publique doit reposer sur une disposition légale, ou en découler. Voir section III.2.5 dudit avis, ainsi que considérant 41 et article 6, paragraphe 3, du règlement général.

¹⁵ Définition de l'indexation:

EXEMPLE: Le rôle des autorités compétentes est d'établir la valeur du patrimoine détenu par l'agent public au début et à la fin de son mandat, et de déterminer comment ce patrimoine a été financé. À cette fin, il peut s'avérer nécessaire de recueillir des informations sur le conjoint et les membres de la famille de l'agent et sur leur patrimoine. Il ne s'ensuit pas pour autant qu'il soit approprié ou proportionné de mettre toutes ces informations à la disposition du public en ligne. Toute incursion dans la vie privée d'une personne doit présenter un caractère de nécessité et de proportionnalité au but légitime poursuivi par le traitement.

3.2.1 PROPORTIONNALITÉ

Le principe de proportionnalité doit être respecté dans toutes les activités de traitement, et en particulier au stade de la collecte des données comme à celui de leur éventuelle publication.

La Cour de justice de l'Union européenne (ci-après la «Cour») a rappelé à plusieurs reprises l'importance d'une approche proportionnée du traitement des données à caractère personnel. Dans les affaires jointes C-465/00, C-138/01 et C-139/01, précitées, la Cour s'est penchée sur cet aspect en s'interrogeant sur le point de savoir *«si l'indication du nom des personnes concernées en regard des revenus perçus est proportionnée au but légitime poursuivi et si les motifs invoqués devant la Cour pour justifier une telle divulgation apparaissent pertinents et suffisants»* (point 86), et a souligné qu'il incombe aux juridictions nationales compétentes de *«vérifier si une telle publicité est, à la fois, nécessaire et proportionnée au but [...] et, en particulier, d'examiner si un tel objectif n'aurait pu être atteint de manière aussi efficace par la transmission des informations nominatives aux seules instances de contrôle»* (point 88). La Cour s'est en outre demandée s'il n'aurait pas été possible de recourir à d'autres moyens, moins susceptibles de porter atteinte à la vie privée des personnes concernées, pour atteindre le but légitime poursuivi¹⁶.

D'autre part, au point 74 de son arrêt dans les affaires jointes C-92/09 et C-93/09, précitées, la Cour a clairement indiqué que, *«[s]elon une jurisprudence constante, le principe de proportionnalité, qui fait partie des principes généraux du droit de l'Union, exige que les moyens mis en œuvre par un acte de l'Union soient aptes à réaliser l'objectif visé et n'aillent pas au-delà de ce qui est nécessaire pour l'atteindre (arrêt du 8 juin 2010, Vodafone e.a., C-58/08, non encore publié au Recueil, point 51 et jurisprudence citée)»*.

Les États membres doivent réfléchir soigneusement au champ d'application personnel des mesures de transparence et de lutte contre les conflits d'intérêts. Pour la détermination des personnes dont les données vont faire l'objet d'un traitement, ils peuvent souhaiter définir des critères objectifs utiles tels que l'autorité publique dont la personne est dépositaire, le pouvoir dont elle dispose pour dépenser ou allouer des fonds publics, son salaire, la durée de son mandat, les avantages et indemnités perçus, etc., en tenant compte de ce que le traitement ne doit pas aller au-delà de ce qui est *«nécessaire à la réalisation des objectifs légitimes*

¹⁶ Dans le contexte en cause, la Cour s'est demandée en particulier *«s'il n'aurait pas été suffisant d'informer le grand public des seuls rémunérations et autres avantages pécuniaires»*. Voir point 88 de l'arrêt Österreichischer Rundfunk (affaires jointes C-465/00 et C-138/01).

poursuivis, eu égard notamment à l'atteinte générée par une telle publication aux droits reconnus par les articles 7 et 8 de la charte»¹⁷.

La publication en ligne d'informations révélant des aspects non pertinents de la vie privée d'une personne n'est pas justifiée au regard des principes de loyauté et de proportionnalité.

❖ Application pratique de la proportionnalité

➤ *Différences entre collecte et publication en ligne de données*

Les mesures de lutte contre les conflits d'intérêts portent généralement sur deux activités principales de traitement: le traitement exclusif, non public, des données à caractère personnel par les institutions compétentes et la publication en ligne de certaines données. Les dispositions légales pertinentes devraient déterminer expressément les personnes qui sont tenues de soumettre des rapports aux institutions compétentes. Elles devraient également préciser quelles sont les données à caractère personnel que doivent contenir ces rapports, et lesquelles doivent être publiées de manière proactive. Le présent avis n'a pas vocation à déterminer quelles sont les données à caractère personnel que devraient collecter les institutions compétentes chargées de la lutte contre les conflits d'intérêts, pas plus qu'il n'entend définir les informations à diffuser en ligne. Il importe néanmoins de souligner que, avant de décider de mettre des informations à la disposition du public en ligne, les institutions compétentes doivent toujours prendre en considération les conséquences d'une telle décision. Il se peut que certaines des données à caractère personnel collectées constituent des informations intimes concernant les agents publics; leur publication en ligne pourrait dès lors avoir de graves effets sur leur vie privée et leurs droits à la protection des données. Il y a lieu également de rappeler que ce qui présente un intérêt pour le public et ce qui est d'intérêt public sont deux choses distinctes.

Les données à caractère personnel mises en ligne tendent à être inférieures en volume à celles communiquées aux institutions compétentes, dans la mesure où la divulgation proactive de certaines informations est susceptible d'être inappropriée, eu égard aux répercussions probables qu'une telle publication aurait sur les personnes concernées. Par ailleurs, certaines des informations non susceptibles d'une publication proactive peuvent être divulguées lorsque des dispositions législatives sur l'accès à l'information trouvent à s'appliquer en vertu de la loi et/ou d'un autre acte législatif pertinent, ou sur décision judiciaire ordonnant leur divulgation. Au moment de déterminer si l'obtention et/ou la publication de données à caractère personnel concernant des agents publics est nécessaire, il convient de vérifier si les affaires et/ou les transactions (financières, contractuelles ou autres) de ces agents n'ont pas eu lieu avant leur entrée en fonctions, alors qu'ils étaient de simples particuliers n'exerçant aucun mandat public. Il n'est pas interdit aux institutions compétentes de collecter des données sur cette base, surtout dans les situations où des activités suspectes ont eu lieu. Néanmoins, la publication en ligne automatique de toutes les affaires/transactions accomplies

¹⁷ Arrêt de la Cour dans les affaires jointes Volker und Markus Schecke GbR (C-92/09) et Hartmut Eifert (C-93/09)/Land Hessen, points 79 et 80.

par les agents publics avant leur entrée en fonctions, interrogeable par nom et contenant tous les détails sans distinction selon la nature, le type et l'étendue des données, risque d'aller au-delà de ce qui est nécessaire pour atteindre les buts légitimes poursuivis.

Avant de publier des données à caractère personnel en ligne, il est indispensable de considérer les risques potentiels d'une telle divulgation. Si l'on envisage une publication systématique ou très détaillée, il est fortement recommandé d'effectuer une analyse d'impact sur la vie privée. Cette analyse devrait également explorer les solutions de rechange possibles pour communiquer certaines données à caractère personnel, telles qu'une communication sous une forme résumée ou agrégée, de façon à ce que les personnes physiques ne puissent pas être identifiées.

Il convient également d'examiner si la nature et l'étendue des données à caractère personnel dont la publication est envisagée sont susceptibles de présenter des risques autres que ceux liés à la protection des données. Par exemple, la publication de données à caractère personnel se rapportant à la situation économique d'une personne concernée peut rendre celle-ci vulnérable face aux criminels. Cela n'exclut pas la divulgation de ces données aux institutions compétentes chargées de la collecte et du traitement de ces données.

De même, avant de prendre la décision de publier des informations concernant les relations contractuelles ou similaires d'un agent public, les institutions compétentes doivent savoir que certaines données pourraient représenter un secret (secret d'affaires, bancaire, professionnel ou autre). En pareil cas, il peut s'avérer nécessaire d'effectuer une pondération entre les droits à la protection des données, la protection du secret et l'intérêt public à l'accès à de telles informations.

EXEMPLE: Les institutions compétentes peuvent collecter les données à caractère personnel du ménage ou des membres de la famille d'un agent public, telles que les noms, coordonnées, adresses, etc., afin de mener à bien leurs missions dans ce domaine; en revanche, la publication en ligne de l'ensemble de ces informations risque de ne pas être proportionnée, bien que chaque cas doive être apprécié individuellement.

➤ *Traitements différenciés selon le groupe de personnes concernées*

Il y a lieu d'adopter une approche sélective pour déterminer le contenu des données à caractère personnel destinées à la publication, en faisant la distinction entre différents groupes de personnes, différents cas de figure et différents objectifs, et en tenant compte des situations particulières. Différentes méthodes devraient être utilisées, selon le cas, pour la mise à disposition des informations.

Au moment d'apprécier si le traitement doit ou non s'étendre à la diffusion publique de données à caractère personnel au moyen de leur publication en ligne, il convient de traiter différemment des situations différentes. Les institutions compétentes pourraient souhaiter prendre en considération la mesure dans laquelle l'institution publique ou l'agent public concernés sont exposés au risque de corruption ou à des situations de conflits d'intérêts, l'étendue des missions ou des fonctions qui leur sont dévolues dans l'intérêt public et le

montant des fonds publics gérés. D'une manière générale, il peut être pertinent de faire la distinction, selon leurs responsabilités hiérarchiques et décisionnelles, entre, premièrement, les responsables politiques, les hauts fonctionnaires ou d'autres personnalités publiques occupant des fonctions qui comportent des responsabilités politiques, deuxièmement, les cadres de la fonction publique, qui n'ont aucun mandat électif et n'exercent que des fonctions de direction ou de gestion, et, troisièmement, les agents publics de base, qui n'ont pas de responsabilités décisionnelles propres.

Dans ce cadre, si, pour le premier groupe, la diffusion en ligne de données à caractère personnel sur le site internet de l'institution compétente concernée peut être considérée comme proportionnée, la même solution risque de ne pas être applicable pour le deuxième ou le troisième groupe. S'agissant du deuxième groupe, le nom et la fonction pourraient être rendus publics, tandis que, par défaut, aucune donnée à caractère personnel concernant les agents ne serait publiée (quand bien même il ne s'agirait que de données à caractère personnel relatives aux actes qu'ils accomplissent en leur qualité d'agents publics ou se rapportant à leurs activités professionnelles¹⁸). Cette recommandation est sans préjudice de la disponibilité de ces données en vertu de la réglementation nationale relative à l'accès du public aux documents.

Il est conseillé, dans le cadre de cette réglementation spécifique, d'opérer une distinction entre les différents groupes d'agents publics, de fonctionnaires et d'autres personnes physiques en fonction des critères précités, et de définir sur cette base plusieurs niveaux d'obligations déclaratives envers les institutions compétentes. Le législateur devrait tenir compte de cette distinction, tout particulièrement pour les éventuelles obligations de publication en ligne.

Cette approche permettrait de moduler le volume et le type de données à caractère personnel communiquées en fonction du groupe de personnes concernées et faciliterait ainsi le respect des exigences de proportionnalité, selon lesquelles le traitement des données à caractère personnel est limité à ce qui est strictement nécessaire pour atteindre le but légitime poursuivi (la détection et la sanction des conflits d'intérêts).

¹⁸ À cet égard, dans son arrêt *Österreichischer Rundfunk* (affaires jointes C-465/00 et C-138/01), la Cour de justice de l'Union européenne attire l'attention sur la jurisprudence de la Cour européenne des droits de l'homme concernant la portée de l'expression «*vie privée*», en rappelant que celle-ci «*ne d[oi]t pas être interprété[e] de façon restrictive*» et qu'«*aucune raison de principe ne permet d'exclure les activités professionnelles [...] de la notion de "vie privée"*». Voir point 73 de l'arrêt.

EXEMPLE: La publication de données à caractère personnel tirées de déclarations d'intérêts remplies par des agents publics exerçant des responsabilités de nature purement administrative a été jugée disproportionnée dans certains cas, compte tenu du fait que ces personnes n'exercent pas de fonctions électives ou ministérielles. En revanche, le dépôt de ces documents auprès des autorités de contrôle compétentes a été considéré comme justifié aux fins de renforcer les garanties d'intégrité et d'impartialité de ces personnes et de prévenir, détecter et sanctionner les situations de conflits d'intérêts¹⁹.

3.2.2 PRINCIPE DE MINIMISATION

Conformément au principe de minimisation, il y a lieu de procéder à une évaluation rigoureuse de la nécessité et de la proportionnalité des données traitées (article 6 de la directive 95/46/CE et dispositions du règlement général). La quantité et le type de données à caractère personnel destinées à être traitées doivent être clairement définis. Les données à caractère personnel appelées à faire l'objet d'un traitement doivent être adéquates, pertinentes et non excessives au regard des finalités spécifiques poursuivies, conformément à la législation, et les informations qui ne sont pas nécessaires pour atteindre ces finalités ne devraient en aucun cas être soumises à traitement. Dans le cadre de la mise en œuvre des mesures de transparence et de lutte contre les conflits d'intérêts, le traitement des données à caractère personnel doit se focaliser sur l'objectif légitime poursuivi et être pertinent au regard de celui-ci, afin d'éviter toute opération de traitement inutile. Le traitement de données n'en sera que plus efficace et plus efficient.

La publication en ligne n'est pas toujours nécessaire pour atteindre la finalité du traitement; dans certains cas, la communication de renseignements d'ordre général sur un domaine précis d'intervention publique ou la présentation, sous la forme d'indicateurs de performance, d'éléments analytiques relatifs à des décisions ou à des actions publiques peuvent suffire. Des données plus approfondies et plus complètes peuvent être communiquées aux autorités de contrôle compétentes, qui se chargeront, au besoin, de mettre ces données en ligne ou de les rendre publiques, en accord avec la réglementation nationale relative à l'accès aux documents publics.

EXEMPLE: Lorsqu'il est nécessaire de collecter et de mettre en ligne des informations sur le patrimoine de personnes proches de l'agent public (telles que le conjoint, les enfants et d'autres membres de la famille ou du ménage), il doit être tenu compte du principe de minimisation pour déterminer si le patrimoine du membre de la famille doit être rendu public sous forme désagrégée ou uniquement dans sa valeur totale. Il importe également d'examiner dans quelle mesure la publication de l'identité de tous les membres de la famille ou du ménage est nécessaire pour atteindre l'objectif poursuivi.

¹⁹ Voir Conseil constitutionnel de la République Française, décision n° 2013-675 DC du 9 octobre 2013 sur la loi organique relative à la transparence de la vie publique (projet de loi adopté le 17 septembre 2013 - TA n° 209).

EXEMPLE: Certaines réglementations nationales relatives à la transparence prévoient la publication en ligne d'informations concernant le montant des rémunérations et des revenus individuels des personnes exerçant de hautes fonctions administratives (par exemple, les titulaires de postes administratifs de haut niveau). En règle générale, pour satisfaire à ces obligations, il peut suffire, conformément au principe de minimisation, de publier le montant total perçu par les personnes concernées. En revanche, il ne serait sans doute pas proportionné de publier des données telles que le numéro d'identification fiscale, des états financiers complets, des informations détaillées tirées des déclarations de revenus ou de la feuille de paie, les coordonnées bancaires, l'adresse du domicile, les numéros de téléphone personnels ou l'adresse électronique privée.

EXEMPLE: S'agissant de la publication en ligne d'informations financières relatives aux personnes concernées (créances, emprunts, etc.), il est recommandé, en vertu du principe de minimisation, de ne publier que les informations nécessaires et/ou élémentaires, en tenant compte de la vulnérabilité de ces données et des risques potentiels découlant de cette divulgation en ligne. Il serait donc souhaitable que la loi précise les modalités de la publication en ligne d'informations financières, afin d'éviter de possibles abus ou la publication excessive de ces données sur l'internet, susceptible d'aller au-delà des buts raisonnables et/ou légitimes poursuivis, eu égard simultanément à l'intérêt public.

❖ Type de données

Lors du traitement de données à caractère personnel au titre des mesures de transparence et de lutte contre les conflits d'intérêts dans le secteur public, l'un des objectifs sera de déterminer si les modifications dans la situation patrimoniale des agents publics sont légitimes. D'une manière générale, toute donnée collectée et/ou publiée doit être fonctionnelle; elle doit servir, par exemple, à déceler si les personnes concernées ont acquis des biens illégalement, ont enfreint une mesure de lutte contre les conflits d'intérêts ou ont commis un acte illicite ou déshonorant. Il n'est pas acceptable de collecter et de traiter des données à caractère personnel qui ne sont pas utiles pour l'appréciation de ces infractions et/ou la détection d'un éventuel comportement répréhensible. Il est recommandé de mettre en place des cadres juridiques et pratiques axés sur la réalisation de la gestion légitime des conflits d'intérêts et de la transparence qui lui est associée, afin de prévenir tout traitement de données inutile, illégitime et abusif.

EXEMPLE: Les relations d'affaires nouées pendant le temps d'exercice du mandat public sont peut-être le signe d'un comportement illicite et pourraient, à ce titre, faire l'objet d'une analyse plus approfondie de la part des institutions compétentes. Il y aura donc lieu de traiter certaines informations dès lors qu'elles sont pertinentes pour vérifier si l'agent public a ou non perçu des gains, financiers ou autres, illicites, que ce soit directement ou indirectement (par l'intermédiaire du conjoint ou d'un membre de la famille).

3.3 TRAITEMENTS PORTANT SUR DES CATÉGORIES PARTICULIÈRES DE DONNÉES À CARACTÈRE PERSONNEL (DONNÉES SENSIBLES)

Conformément à l'article 8, paragraphe 1, de la directive 95/46/CE, les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques et l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle appartiennent à des catégories particulières. Le règlement général étend les catégories particulières de données à caractère personnel aux données génétiques, aux données biométriques, servant à l'identification unique d'une personne physique, et aux données concernant l'orientation sexuelle. Tant la directive 95/46/CE que le règlement général prévoient que le traitement de ces données est interdit en règle générale, tout en définissant plusieurs exceptions où leur traitement est admis.

D'autre part, l'article 8, paragraphe 5, de la directive 95/46/CE dispose que le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Une disposition similaire a été insérée dans le règlement général.

Compte tenu des dispositions précitées, une divulgation proactive de ces données ne peut intervenir qu'à titre exceptionnel, sur le fondement d'une base juridique spécifique et en opérant toujours une pondération équilibrée entre la protection de la vie privée et l'intérêt public légitime.

EXEMPLE: Si la procédure de candidature l'impose, on peut admettre la publication d'informations relatives à des élus représentant des partis politiques qui révélerait leurs liens avec certains groupes politiques ou certaines organisations syndicales.

3.4 DURÉE DE CONSERVATION

Le délai de conservation des données à caractère personnel sous une forme permettant l'identification des personnes concernées doit être déterminé en fonction des finalités légitimes pour lesquelles elles sont conservées. Les données ne peuvent faire l'objet d'un traitement que pendant la période nécessaire pour la réalisation de ces finalités légitimes. Le traitement au sein des institutions compétentes doit être considéré indépendamment de l'objectif recherché par la publication des données à caractère personnel. Il est préférable que les délais de conservation soient clairement indiqués et qu'ils comportent également des dispositions sur la durée de mise en ligne.

Différentes étapes peuvent être définies: délai de traitement des données pour la réalisation de l'objectif principal, durée de publication des données et, le cas échéant, durée d'archivage. Il est aussi envisageable de prévoir des durées différentes selon les données ou ensembles de données.

3.5 EXACTITUDE DES DONNÉES

Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour. Conformément à l'article 6 de la directive 95/46/CE, toutes les mesures raisonnables doivent être prises pour garantir l'exactitude et l'actualité des données, au regard des finalités pour

lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. D'autre part, à la lumière du règlement général, l'agent public a le droit d'obtenir des institutions compétentes, dans les meilleurs délais, la rectification des données à caractère personnel le concernant qui sont inexactes ou obsolètes. L'article 16 du règlement général prévoit en outre que, compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

Lorsque la loi impose que certaines données soient mises en ligne, il est conseillé aux institutions compétentes, en considération du principe d'exactitude, de créer un ou des formulaires/déclarations uniques, clairement conçus, qui ne contiendraient que les données pertinentes.

Il est également recommandé que les institutions compétentes mettent en place les procédures appropriées pour assurer l'exactitude et l'actualité des données à caractère personnel collectées, en application de l'article 6 de la directive 95/46/CE et à la lumière du règlement général. Il est de bonne pratique d'indiquer la date de publication ou de dernière mise à jour sur les ensembles de données publiés.

3.6. LIMITATION DE LA FINALITÉ

Les données collectées ne peuvent être traitées qu'à des fins déterminées et à d'autres fins compatibles. Aux termes de l'article 6, paragraphe 1, point b), de la directive 95/46/CE, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

De même, une disposition similaire du règlement général prévoit que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités; 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 comme incompatible avec les finalités initiales.

Il est à noter que, dans plusieurs États membres de l'Union, certains responsables du traitement ont ajouté des informations spécifiques pour expliquer les limites de la réutilisation des données publiées. En effet, comme le GT 29 l'a souligné dans son avis 6/2013 sur la réutilisation des informations du secteur public et des données ouvertes, les réutilisateurs potentiels sont tenus de se conformer à la législation sur la protection des données, en tant que responsables du traitement, lorsqu'ils manient des données à caractère personnel, à moins que leurs activités de traitement ne soient couvertes par l'exemption domestique prévue à l'article 3 de la directive 95/46/CE.

Pour décider si les données à caractère personnel doivent être accessibles mondialement par des moteurs de recherche externes, il convient de ne pas perdre de vue l'objectif qui est poursuivi en mettant ces informations à la disposition du plus grand nombre. Si la mise à disposition de ces données présente un intérêt public mondial, compte tenu surtout de la

catégorie de personnes concernées, une telle diffusion est susceptible d'être justifiée. Cela sous réserve que les éventuelles répercussions sur les droits et libertés des personnes concernées aient été prises en compte. En revanche, en l'absence d'intérêt public mondial, ou lorsqu'une diffusion aussi large apparaît comme inappropriée, il peut être préférable de limiter l'accessibilité des données à des moteurs de recherche internes²⁰ ou de recourir à d'autres mécanismes d'accès sélectif (par exemple, authentification avec nom d'utilisateur ou captcha).

Il est recommandé que la réutilisation des données soit expressément autorisée ou interdite, et que, le cas échéant, les conditions de leur réutilisation soient précisées²¹.

4. MESURES DE SÉCURITÉ

Les institutions compétentes, en leur qualité de responsables du traitement, doivent mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés ainsi que contre toute autre forme de traitement illicite. Les mesures de protection doivent être adaptées à la nature des activités de traitement réalisées par les institutions compétentes.

À cette fin, il convient de prendre les mesures appropriées pour réduire le risque que les informations et les documents disponibles sur l'internet puissent être effacés, modifiés, dénaturés et/ou sortis de leur contexte; par exemple, il est envisageable d'indiquer des sources fiables pour l'obtention des documents, d'utiliser des signatures électroniques pour garantir l'authenticité et l'intégrité des documents, ou encore d'insérer des «données contextuelles» dans les fichiers mis en ligne sur les sites internet officiels (informations sur la version, date d'expiration, organe administratif responsable, etc.).

5. DROITS DES PERSONNES CONCERNÉES

Afin de garantir un traitement loyal des données, le GT 29 recommande que les institutions compétentes informent tout réutilisateur éventuel de ses obligations en lien avec les droits des personnes concernées et de la manière de s'y conformer.

Préalablement à la collecte de données à caractère personnel, les institutions compétentes doivent informer l'agent public concerné, en application des articles 10 et 11 de la directive 95/46/CE. Le droit d'être informé peut découler de la législation pertinente établissant les données personnelles qui doivent être rendues publiques et dont la publication ne nécessite donc pas le consentement préalable de l'agent public concerné.

²⁰ À cet effet, il est possible de coder des règles d'accès spécifiques dans chaque fichier texte (par exemple, à l'aide des balises méta noindex/noarchive et du fichier robots.txt, à configurer selon le protocole d'exclusion des robots). Cela s'entend sans préjudice de l'utilisation d'outils pouvant faciliter l'extraction d'informations ou de documents diffusés sur le site internet officiel d'un organisme public.

²¹ Voir avis 6/2013 du groupe de travail «article 29» (WP207).

En outre, la personne concernée a le droit d'obtenir des institutions compétentes les informations suivantes, sauf exception prévue par la directive 95/46/CE:

- la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées;
- la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données;
- la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées.

Conformément à l'article 14 de la directive 95/46/CE, la personne concernée a le droit, dans certains cas²², de s'opposer à tout moment à ce que des données la concernant fassent l'objet d'un traitement. Il est recommandé que le responsable du traitement informe de cette opposition tous les réutilisateurs éventuels de ces données²³.

Ce droit d'opposition peut faire l'objet d'une renonciation ou de restrictions en vertu de la loi, selon la finalité poursuivie. Par exemple, les personnes concernées pourront s'opposer, pour des raisons prépondérantes et légitimes tenant à leur situation particulière, à la publication en ligne de certaines ou de la totalité des données les concernant, mais pas à leur traitement interne (distinct de la diffusion de données les concernant).

De même, toute personne concernée est en droit d'obtenir des institutions compétentes la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la directive 95/46/CE. En outre, toute rectification, tout effacement ou tout verrouillage est notifié aux tiers auxquels les données ont été communiquées, si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.

En vertu du règlement général, la personne concernée dispose du droit de rectification, du droit à l'effacement, du droit à la limitation du traitement ainsi que du droit d'introduire une réclamation auprès d'une autorité de protection des données.

²² À cet égard, il y a lieu de rappeler que l'article 14 de la directive prévoit que la personne concernée peut exercer son droit d'opposition au moins, notamment, dans le cas visé à l'article 7, point e), de la directive. Cela signifie que, lorsque le traitement est autorisé à la suite d'une évaluation raisonnable et objective des différents droits et intérêts en jeu, la personne concernée dispose encore d'une possibilité supplémentaire de marquer son opposition, pour des motifs liés à sa situation particulière. Voir avis 06/2014 du GT 29, précité, section III.3.6.

²³ En France, il s'agit d'une obligation en vertu de l'article 97 du décret d'application de la loi Informatique et libertés.