

CONSEIL DE L'EUROPE

COMITÉ DES MINISTRES

RECOMMANDATION N° R (91) 10

DU COMITÉ DES MINISTRES AUX ÉTATS MEMBRES

SUR LA COMMUNICATION À DES TIERCES PERSONNES DE DONNÉES À CARACTÈRE PERSONNEL DÉTENUES PAR DES ORGANISMES PUBLICS¹

*(adoptée par le Comité des Ministres le 9 septembre 1991,
lors de la 461^e réunion des Délégués des Ministres)*

Le Comité des Ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Notant que l'informatique a permis aux organismes publics d'enregistrer des données dans des fichiers électroniques, y compris des données à caractère personnel, qu'ils collectent en vue d'exercer leurs fonctions ;

Conscient du fait que les nouvelles techniques automatisées d'enregistrement de telles données facilitent grandement l'accès de tierces personnes à ces données, contribuant ainsi à une circulation plus large de l'information au sein de la société, que le Comité des Ministres a encouragée dans sa Recommandation n° R (81) 19 sur l'accès à l'information détenue par les autorités publiques ainsi que par sa Déclaration du 29 avril 1982 sur la liberté d'expression et d'information ;

Estimant cependant que l'automatisation des données collectées et enregistrées par les organismes publics implique la nécessité de prendre en compte son impact sur les données à caractère personnel ou sur les fichiers contenant des données à caractère personnel collectées et enregistrées par des organismes publics en vue d'exercer leurs fonctions ;

Notant en particulier que l'automatisation des fichiers contenant des données à caractère personnel a augmenté le risque d'ingérence dans la vie privée, étant donné qu'elle permet un plus grand accès, par des moyens télématiques, aux données à caractère personnel contenues dans les fichiers détenus par les organismes publics, ainsi qu'une communication de ces données à caractère personnel ou de ces fichiers à des tierces personnes ;

Ayant à l'esprit à cet égard la tendance croissante du secteur privé à exploiter, à des fins commerciales, les données à caractère personnel ou les fichiers contenant des données à caractère personnel

1. Lors de l'adoption de cette recommandation, et en application de l'article 10.2.c du Règlement intérieur des réunions des Délégués des Ministres :

- le Délégué de l'Irlande a réservé le droit de son Gouvernement de se conformer ou non aux principes 6.2, 6.3, paragraphe 2, et 7.1 de l'annexe à la recommandation ;
- les Délégués de la Norvège et du Royaume-Uni ont réservé le droit de leur Gouvernement de se conformer ou non aux principes 6.2 et 6.3, paragraphe 2, de l'annexe à la recommandation ;
- le Délégué de la Suède a réservé le droit de son Gouvernement de se conformer ou non au principe 6.2 de l'annexe à la recommandation.

détenus par des organismes publics, ainsi que l'apparition de pratiques des organismes publics visant à communiquer, par le truchement de moyens électroniques, des données à caractère personnel ou des fichiers contenant des données à caractère personnel à des tierces personnes sur une base commerciale ;

Déterminé en conséquence à promouvoir les principes de protection des données établis par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel¹, afin d'assurer que la communication de données à caractère personnel ou de fichiers contenant des données à caractère personnel par des organismes publics à des tierces personnes, en particulier par des moyens électroniques, repose sur des fondements juridiques et soit entourée de garanties pour la personne concernée ;

Notant en particulier que ces principes de protection des données devraient se refléter dans le nouveau contexte informatique qui caractérise désormais la communication de données à caractère personnel ou de fichiers contenant des données à caractère personnel à des tierces personnes, selon les dispositions juridiques régissant l'accessibilité aux tierces personnes des données à caractère personnel ou des fichiers contenant des données à caractère personnel,

Recommande aux gouvernements des Etats membres :

i. de tenir compte des principes contenus dans l'annexe à la présente recommandation chaque fois que des données à caractère personnel ou des fichiers contenant des données à caractère personnel collectées et enregistrées par les organismes publics peuvent être accessibles à des tierces personnes ;

ii. de tenir dûment compte des principes contenus dans l'annexe à la présente recommandation dans leur droit et leur pratique concernant l'automatisation et la communication à des tierces personnes, par des moyens électroniques, de données à caractère personnel ou de fichiers contenant des données à caractère personnel ;

iii. d'assurer une large diffusion au sein des organismes publics des principes contenus dans l'annexe à la présente recommandation ;

iv. de porter les principes contenus dans l'annexe à la présente recommandation à l'attention des autorités établies en vertu d'une législation sur la protection des données ou d'une législation sur l'accès à l'information du secteur public.

Annexe à la Recommandation n° R (91) 10

1. *Champ d'application et définitions*

1.1. Les principes contenus dans la présente recommandation s'appliquent au traitement automatisé de données à caractère personnel collectées par des organismes publics et pouvant faire l'objet d'une communication à des tierces personnes.

1.2. Les Etats membres peuvent étendre le champ d'application de la présente recommandation de façon à inclure les données relatives aux groupements, compagnies, associations, etc., dotés ou non de la personnalité juridique, ainsi que les données à caractère personnel sous forme non automatisée.

Aux fins de la présente recommandation :

1.3. — l'expression « données à caractère personnel » désigne toute information concernant une personne identifiée ou identifiable (personne concernée) ; une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais, des coûts et des activités déraisonnables ;

— l'expression « organismes publics » désigne toute administration, institution, établissement ou autre entité qui exerce des fonctions de service public ou d'intérêt public au moyen de privilèges de puissance publique.

1. Strasbourg, 1981, Série des traités européens n° 108 (ci-après dénommée la Convention n° 108).

Le droit interne peut élargir la portée de l'expression « organismes publics ».

— l'expression « fichiers accessibles à des tierces personnes » désigne les fichiers détenus par des organismes publics et contenant des données à caractère personnel pouvant être communiquées au public ou à des tierces personnes, ayant un intérêt particulier et qui sont en conformité avec la législation générale sur l'accès à l'information du secteur public ou sur la liberté d'information, les dispositions constitutionnelles ainsi que les lois spécifiques, les règlements ou la jurisprudence autorisant des tierces personnes à avoir accès aux informations détenues par des organismes publics, y compris au moyen d'une publication officielle ;

— l'expression « communication » désigne le fait de rendre des fichiers ou des données à caractère personnel accessibles, notamment en autorisant leur consultation, leur transmission, leur diffusion ou leur mise à disposition quels que soient les moyens ou les supports utilisés ;

— l'expression « tierces personnes » désigne toute personne physique ou morale à laquelle les données à caractère personnel sont communiquées par les organismes publics à l'exclusion d'autres organismes publics.

Le droit interne peut élargir la portée de l'expression « tierces personnes ».

2. *Respect de la vie privée et principes de protection des données*

2.1. La communication par des organismes publics, en particulier par des moyens électroniques, de données à caractère personnel ou de fichiers contenant des données à caractère personnel à des tierces personnes devrait être accompagnée de sauvegardes et de garanties destinées à assurer que la vie privée de la personne concernée ne sera pas indûment affectée.

En particulier, la communication de données à caractère personnel ou de fichiers contenant des données à caractère personnel à des tierces personnes ne devrait avoir lieu que si :

- a. une loi spécifique le prévoit ; ou
- b. le public y a accès en vertu d'une disposition juridique régissant l'accès à l'information du secteur public ; ou
- c. la communication est conforme à la législation interne sur la protection des données ; ou
- d. la personne concernée a donné son consentement exprès et éclairé.

2.2. A moins que le droit interne n'organise des sauvegardes et garanties appropriées en faveur de la personne concernée, les données à caractère personnel ou les fichiers contenant des données à caractère personnel ne doivent pas être communiqués à des tierces personnes à des fins incompatibles avec celles pour lesquelles les données ont été collectées.

2.3. La législation interne sur la protection des données devrait s'appliquer au traitement par une tierce personne des données à caractère personnel qui lui sont communiquées par des organismes publics.

3. *Données sensibles*

3.1. Les données à caractère personnel entrant dans l'une des catégories des données sensibles énoncées à l'article 6 de la Convention n° 108 ne devraient pas être enregistrées dans un fichier ou dans la partie d'un fichier généralement accessibles à des tierces personnes.

Toute exception à ce principe devrait être strictement prévue par la loi et accompagnée des garanties et sauvegardes appropriées en faveur de la personne concernée.

3.2. Les dispositions du principe 3.1 ne portent pas préjudice à la possibilité d'enregistrer dans des fichiers accessibles à des tierces personnes des catégories de données — qui dans d'autres circonstances pourraient être considérées comme sensibles — relatives à la vie publique des personnes lorsque ces personnes ont une activité relevant du domaine public et que, de ce fait, elles rendent leurs données accessibles à des tierces personnes.

4. *Données généralement accessibles*

4.1. Les finalités pour lesquelles les données seront collectées et traitées dans des fichiers accessibles à des tierces personnes ainsi que l'intérêt public justifiant leur accessibilité devraient être indiqués conformément au droit et à la pratique internes.

4.2. La personne concernée devrait, avant ou lors de la collecte, être informée, conformément au droit et à la pratique internes, du caractère obligatoire ou facultatif de la collecte, des fondements juridiques et de la finalité de la collecte et du traitement des données à caractère personnel, ainsi que de l'intérêt public qui justifie leur accessibilité.

4.3. Les organismes publics devraient pouvoir éviter que les données à caractère personnel enregistrées dans un fichier accessible au public et relatives à des personnes dont la sécurité et la vie privée sont particulièrement menacées soient communiquées à des tierces personnes.

5. Accès et communication de données à caractère personnel par le biais de moyens électroniques

5.1. Le traitement automatisé des données à caractère personnel contenues dans des fichiers accessibles à des tierces personnes devrait être réalisé en conformité avec le droit interne.

Celui-ci devrait fixer les conditions qui régissent la communication et l'accès aux données, et, en particulier, couvrir la communication automatique et la consultation en ligne de ces données.

5.2. Lors de la communication automatique, des moyens techniques propres à limiter la portée des interrogations et des recherches électroniques devraient être mis en place en vue de prévenir tout téléchargement ou consultation non autorisés de données à caractère personnel ou de fichiers contenant de telles données.

6. Traitement par des tierces personnes de données à caractère personnel provenant de fichiers accessibles à des tierces personnes

6.1. Lorsque la personne concernée est juridiquement tenue de fournir ses données pour enregistrement dans un fichier accessible à des tierces personnes, le traitement des données par des tierces personnes devrait soit être assujéti au consentement exprès et éclairé de la personne concernée, soit être conforme aux prescriptions de la loi.

Lorsque le consentement est requis, la personne concernée devrait pouvoir le retirer à tout moment.

6.2. Si l'enregistrement des données dans un fichier accessible à des tierces personnes est facultatif, la personne concernée devrait, avant ou lors de la collecte, être informée de son droit :

- a. de ne pas faire enregistrer ses données dans un fichier accessible à des tierces personnes, ou
- b. de les faire enregistrer dans un tel fichier et les communiquer sans qu'elles puissent être traitées par des tierces personnes, ou
- c. de s'opposer à ce qu'elles continuent à être traitées par des tierces personnes, ou
- d. de les faire effacer à tout moment.

6.3. Si une tierce personne crée des fichiers contenant des données à caractère personnel issues de fichiers accessibles à des tierces personnes, ces fichiers devraient être soumis aux exigences de la législation interne sur la protection des données, y compris aux droits de la personne concernée.

En particulier, la personne concernée devrait pouvoir connaître l'existence et les finalités du nouveau fichier, et son droit de faire effacer ses données du fichier en question.

7. Appariement-mise en relation de fichiers

Sauf si le droit interne le permet et fournit des garanties appropriées, la mise en relation — notamment par connexion, fusion ou téléchargement — de données à caractère personnel issues de fichiers constitués de données à caractère personnel accessibles à des tierces personnes, en vue de créer de nouveaux fichiers, ainsi que la mise en relation ou l'appariement de fichiers ou de données détenus par des tierces personnes avec un ou plusieurs fichiers détenus par des organismes publics, en vue d'enrichir des fichiers ou des données existants, devraient être interdits.

8. Flux transfrontières de données

8.1. Les principes de la présente recommandation sont applicables à la communication transfrontière de données à caractère personnel collectées par des organismes publics, qui peuvent être communiquées à des tierces personnes.

8.2. La communication transfrontière de données à caractère personnel à des tierces personnes résidant dans un Etat ayant ratifié la Convention n° 108 et disposant ainsi d'une législation sur la protection des données ne devrait pas être soumise à des conditions particulières de protection de la vie privée.

8.3. Lorsque le respect du principe de la protection équivalente est assuré, il ne devrait pas y avoir de limitation à la communication transfrontière de données à caractère personnel à des tierces personnes résidant dans un Etat n'ayant pas ratifié la Convention n° 108, mais jouissant de dispositions juridiques conformes aux principes de ladite convention et de la présente recommandation.

8.4. A moins que le droit interne n'en dispose autrement, la communication transfrontière de données à caractère personnel à des tierces personnes résidant dans un Etat n'ayant pas de dispositions juridiques conformes à la Convention n° 108 et à la présente recommandation ne devrait en règle générale pas intervenir, à moins :

- a. que des mesures nécessaires, y compris de nature contractuelle, au respect des principes de la convention et de la présente recommandation n'aient été prises et que la personne concernée n'ait la possibilité de s'opposer à la communication, ou
- b. que la personne concernée n'ait donné son consentement écrit, exprès et éclairé, et qu'elle n'ait la possibilité de retirer son consentement en tout temps.

8.5. Des mesures devraient être prises afin d'éviter que des données à caractère personnel ou des fichiers contenant de telles données puissent faire l'objet d'une communication transfrontière automatique à des tierces personnes à l'insu des personnes concernées.

9. *Coordination-coopération*

Lorsqu'une législation générale régissant l'accès à l'information du secteur public prévoit l'établissement d'un organe de contrôle pour mettre en œuvre une telle législation et lorsqu'il existe aussi une législation générale sur la protection des données créant une autorité distincte responsable de la mise en œuvre de cette législation, les autorités respectives devraient s'entendre pour faciliter l'échange de l'information concernant les conditions régissant la communication des données à caractère personnel provenant de fichiers accessibles à des tierces personnes.