CONSEIL DE L'EUROPE
COMITÉ DES MINISTRES

RECOMMANDATION N° R (90) 19

DU COMITÉ DES MINISTRES AUX ÉTATS MEMBRES

SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL UTILISÉES À DES FINS DE PAIEMENT ET AUTRES OPÉRATIONS CONNEXES[1]

(adoptée par le Comité des Ministres le 13 septembre 1990, lors de la 443e 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 ;

Conscient de l'utilisation croissante du traitement automatisé de données dans le secteur des moyens de paiement et autres opérations connexes, et des avantages qu'elle présente ;

Conscient de l'utilisation croissante du traitement automatisé de données par des organismes fournissant des services financiers qui ne sont pas nécessairement des banques ;

Estimant que l'utilisation du traitement automatisé de données dans le secteur des moyens de paiement et autres opérations connexes pourrait entraîner des risques pour la vie privée de l'individu ;

Estimant d'ailleurs que, nonobstant l'utilisation croissante du traitement automatisé des données dans le secteur des moyens de paiement et autres opérations connexes, l'individu ne devrait pas être contraint d'utiliser un moyen de paiement électronique, bénéficiant ainsi de la possibilité de maintenir à un minimum les données à caractère personnel qui sont divulguées lors des transactions ;

Reconnaissant que les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 s'appliquent aux activités de traitement automatisé des données par des organismes fournissant des services financiers ;

Estimant néanmoins qu'il convient de préciser les dispositions générales de la convention pour les adapter aux exigences particulières des catégories d'opérations mentionnées plus haut ;

Ayant à l'esprit le caractère international de certaines opérations et les flux transfrontières de données personnelles qu'elles engendrent, qui requièrent la promotion d'une protection des données personnelles équivalente dans tous les Etats membres du Conseil de l'Europe,

Recommande aux gouvernements des Etats membres :

— de tenir compte, dans leurs droit et pratique internes relatifs au secteur des moyens de paiement et autres opérations connexes, des principes et des lignes directrices énoncés dans l'annexe à la présente recommandation ;

---

1. Lors de l'adoption de cette recommandation, le Délégué du Royaume-Uni, en application de l'article 10.2.*c* du Règlement intérieur des réunions des Délégués des Ministres, a réservé le droit de son gouvernement de se conformer ou non aux paragraphes 3.3, 3.4, 5.1.*c* et 7.1 de l'annexe à la recommandation.

— d'assurer une large diffusion de la présente recommandation auprès des autorités compétentes dans le domaine de la protection des données et auprès des organismes fournissant des moyens de paiement, des bénéficiaires et des exploitants de réseaux de communications, ou de leurs représentants.

Annexe à la Recommandation n° R (90) 19

1. *Champ d'application et définitions*

1.1. Les principes énoncés dans la présente recommandation s'appliquent au traitement automatisé de données à caractère personnel liées à la fourniture et à l'utilisation d'un moyen de paiement ou d'autres opérations connexes.

En outre, ces principes s'appliquent à l'ensemble des parties à ces opérations (bénéficiaires, organismes fournissant des moyens de paiement et exploitants de réseaux de communications).

1.2. Aux fins de la présente recommandation :

L'expression « données à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais, des coûts et des activités déraisonnables.

L'expression « moyen de paiement » recouvre l'ensemble des instruments de paiement et autres supports des ordres de paiement, en particulier les chèques, ordres de virement et cartes de paiement, ainsi que tout autre type d'ordres de débit ou de crédit, qu'ils soient ou non initiés par un message électronique.

L'expression « bénéficiaire » comprend l'ensemble des personnes physiques ou morales qui bénéficient d'un paiement ou d'une autre opération connexe, en particulier les commerçants, les détaillants, les prestataires de services, à l'exclusion des consommateurs individuels.

L'expression « organismes fournissant des moyens de paiement » recouvre l'ensemble des entreprises bancaires et non bancaires qui fournissent ou gèrent des moyens de paiement régulièrement ou ponctuellement.

Sont également comprises les entreprises qui reçoivent mandat de la part de l'organisme fournisseur principal de fournir ou de gérer des moyens de paiement.

L'expression « exploitant du réseau de communications » se réfère à l'organisme qui fournit le support de transmission des données utilisées pour l'exécution du paiement ou de l'opération connexe.

2. *Respect de la vie privée*

Le respect de la vie privée des individus doit être garanti lors de la collecte, de l'enregistrement, de l'utilisation, de la communication et de la conservation des données à caractère personnel liées à la fourniture ou à l'utilisation d'un moyen de paiement. A cet effet, les organismes fournissant des moyens de paiement, les bénéficiaires et les exploitants du réseau de communications doivent prendre les mesures nécessaires pour assurer la confidentialité de ces données à caractère personnel.

3. *Collecte et enregistrement des données*

3.1. Pour la fourniture d'un moyen de paiement, les données à caractère personnel ne devraient être collectées et enregistrées par l'organisme fournissant ce moyen de paiement que lorsque ces données sont nécessaires à la mise à disposition du moyen de paiement et des services liés à son utilisation, y compris à des fins de contrôle.

3.2. Conformément aux dispositions du droit interne, l'organisme fournissant un moyen de paiement devrait pouvoir confier la collecte, l'enregistrement et le traitement de ces données à un mandataire dans la mesure où celui-ci s'engage à ne pas les utiliser à d'autres fins.

3.3. En principe, les données à caractère personnel devraient être collectées uniquement auprès de la personne concernée. Lorsque la consultation d'autres sources se révèle nécessaire, l'individu devrait au préalable être pleinement informé des catégories de sources pouvant être consultées et des conséquences pouvant résulter d'un refus ou d'un retrait de consentement.

3.4. Les données à caractère personnel ne devraient pouvoir être collectées et enregistrées par le bénéficiaire qu'à des fins de vérification de l'identité du titulaire du moyen de paiement et de détermination de la validité ou du caractère licite de l'opération de paiement, ou autre opération connexe.

3.5. Lorsqu'une opération est réalisée à l'aide du moyen de paiement, les données personnelles liées à cette opération ne devraient être collectées et enregistrées par l'organisme fournissant les moyens de paiement que dans la mesure où elles sont nécessaires à la validité et à la preuve de l'opération, ainsi qu'à la réalisation des services et à la prise en compte de toute obligation découlant du droit interne liée à son utilisation.

3.6. Les systèmes de paiement devraient être conçus de façon à éviter que, pour une opération de paiement ou autre opération connexe, les données à caractère personnel qui ne sont pas nécessaires à la réalisation des objectifs décrits dans les principes 3.1 et 3.5 soient communiquées à l'organisme fournissant un moyen de paiement, et que les données à caractère personnel qui ne sont pas nécessaires à la réalisation des objectifs décrits dans le principe 3.4 soient conservées par le bénéficiaire.

3.7. L'exploitant du réseau de communications devrait pouvoir collecter et enregistrer uniquement les données à caractère personnel nécessaires à l'exécution, à la preuve et à la facturation des services qu'il fournit.

3.8. Le traitement des données à caractère personnel relatives aux condamnations pénales d'un individu ne devrait être réalisé que lorsque les données sont telles qu'elles sont vraiment justifiées pour déterminer s'il est opportun que cet individu reçoive ou continue d'utiliser un moyen de paiement et dans la mesure où il a donné son consentement exprès et éclairé, ou à condition que le traitement soit conforme aux garanties établies par le droit interne.

La collecte et l'enregistrement des autres catégories de données sensibles mentionnées à l'article 6 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ne devraient pas être permis.

4. *Utilisation des données*

4.1. Sous réserve des dispositions du principe 4.2, les données à caractère personnel collectées et enregistrées conformément au principe 3 ne devraient être utilisées que pour déterminer si un moyen de paiement peut être fourni à une personne qui en fait la demande, pour effectuer des contrôles, pour gérer le compte concerné, y compris la délivrance de relevés bancaires, ou pour éviter des abus en cas de perte ou de révocation du moyen de paiement.

4.2. Pour autant que l'intéressé ait été pleinement informé par écrit et sauf objection de sa part, l'organisme fournissant des moyens de paiement peut utiliser, à des fins de marketing et de promotion de sa gamme de services, les données collectées et enregistrées aux fins énoncées aux principes 3.1 et 3.5.

L'individu devrait être informé du fait que, s'il soulève une objection à ce que ses données soient utilisées à des fins de marketing ou de promotion, cela ne devrait pas nuire à la décision de lui fournir un moyen de paiement ou de lui permettre de continuer à utiliser un moyen de paiement déjà délivré.

4.3. L'interconnexion de différents fichiers de données à caractère personnel découlant des diverses utilisations du moyen de paiement par l'individu ne devrait être effectuée par l'organisme fournissant le moyen de paiement qu'aux fins énoncées au principe 4.1 ou aux fins de marketing et de mise à disposition de services, que l'individu a acceptées conformément au principe 4.2.

A l'exception de situations régies par le droit interne ou si l'individu a donné son consentement exprès et éclairé, l'interconnexion des différents fichiers de données à caractère personnel à des fins autres que celles énoncées dans ce principe ne devrait pas être permise.

4.4. Dans la mesure où l'utilisation d'un moyen de paiement engendre des données sensibles, celles-ci ne doivent pas être utilisées à des fins de marketing ou de promotions ou à toute autre fin.

4.5. Lorsqu'une carte multifonctionnelle constitue entre autres un moyen de paiement et est utilisée à d'autres fins que celles citées au principe 1.2, deuxième alinéa, elle devrait être conçue de manière à rendre impossible l'accès aux données à caractère personnel couvertes par la présente recommandation lorsqu'elle est utilisée à d'autres fins.

5. *Communication des données*

5.1. Les données à caractère personnel collectées et enregistrées aux fins énoncées aux principes 3.1 et 4.1 ne peuvent être communiquées que dans les cas suivants :

a. conformément aux obligations prévues par le droit interne ;

b. lorsqu'il est nécessaire de protéger les intérêts essentiels et légitimes de l'organisme fournissant le moyen de paiement ;

c. lorsque l'individu concerné a donné son consentement exprès et éclairé ;

d. en cas d'incident de paiement, lorsqu'un système de communication ou d'enregistrement de telles informations a été mis sur pied conformément au droit interne, en vue d'accroître la sécurité du paiement dans le secteur couvert par cette recommandation.

5.2. Les conditions posées par le principe 5.1 ne font pas obstacle à la communication des données à caractère personnel par l'organisme fournissant le moyen de paiement à des mandataires agissant en son nom et à l'exploitant du réseau de communications dans la mesure où cette communication est nécessaire à l'octroi et à l'utilisation du moyen de paiement.

6. *Publicité*

Conformément au droit et à la pratique internes, les organismes fournissant des moyens de paiement ainsi que les bénéficiaires et les exploitants du réseau de communications devraient assurer l'information des personnes concernées sur la nature des données qu'ils enregistrent, sur les fins pour lesquelles les données sont enregistrées, sur les catégories de personnes ou d'organismes auxquelles les données peuvent être communiquées et sur le fondement juridique d'une telle communication.

7. *Droits d'accès et de rectification*

7.1. Toute personne devrait, sur demande, pouvoir obtenir sous forme compréhensible toutes données la concernant, y compris celles figurant sur un moyen de paiement.

7.2. Toute personne devrait pouvoir faire rectifier ou effacer de telles données lorsqu'elles sont inexactes, non pertinentes, excessives, ou lorsqu'elles ont été collectées ou enregistrées en contravention avec les principes énoncés dans la présente recommandation.

7.3. Les organismes fournissant des moyens de paiement devraient prendre des mesures adéquates pour assurer que la personne concernée est consciente de ses droits prévus aux principes 7.1 et 7.2 à l'égard des données la concernant, ainsi que des voies et moyens de les exercer.

7.4. L'organisme fournissant des moyens de paiement devrait veiller à ce que la personne concernée puisse exercer son droit d'accès sans délais ou redevances excessifs, en particulier lorsqu'une décentralisation d'un système de traitement de données implique une dissémination des données vers plusieurs fichiers.

8. *Sécurité des données*

8.1. Toute partie aux opérations de paiement ou autres opérations connexes devrait prendre les mesures organisationnelles et techniques appropriées afin de préserver la sécurité, l'intégrité et la confidentialité des données à caractère personnel contre tout accès, utilisation, communication, modification ou détournement non autorisés.

8.2. Des mesures de contrôle suffisantes pour garantir la protection de ces données devraient être prévues par chacun des bénéficiaires, des organismes fournissant des moyens de paiement et des exploitants de réseaux de communications.

En particulier, ces derniers devraient informer leur personnel de telles mesures et de la nécessité de les respecter. Des mesures devraient être prises au sein de l'organisation afin d'identifier clairement les membres du personnel qui ont le droit d'accéder aux données.

8.3. Les organismes fournissant des moyens de paiement devraient donner des conseils en matière de sécurité aux clients, y compris des conseils sur la façon d'utiliser en toute sécurité les moyens de paiement et les codes, et sur la procédure à suivre en cas de perte ou de vol de ces moyens de paiement.

9. *Recours*

Le droit interne devrait prévoir des recours pour toute violation des principes de base des dispositions de la présente recommandation, en particulier lorsque les droits prévus au principe 7 ne sont pas respectés.

10. *Flux transfrontières de données*

10.1. Lorsque la fourniture ou l'utilisation d'un moyen de paiement nécessite la collecte, l'enregistrement ou le traitement de certaines données à caractère personnel dans deux ou plusieurs Parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, il ne devrait y avoir d'obstacle aux flux transfrontières de telles données entre les Parties, pour autant que le principe de la protection équivalente soit garanti.

10.2. Si l'Etat vers lequel les données seront transférées n'est pas Partie à la convention, le respect par cet Etat des principes contenus dans la présente recommandation doit être considéré, par les autorités compétentes des Parties contractantes, comme une forte justification pour permettre le transfert des données à caractère personnel vers cet Etat.

11. *Conservation des données*

11.1. Lorsque des données à caractère personnel ne sont plus nécessaires à l'accomplissement des fins prévues par la présente recommandation, elles devraient être supprimées.

11.2. Les mandataires habilités à traiter des données pour le compte d'un organisme fournissant des moyens de paiement ne devraient pas les conserver au-delà du temps nécessaire à l'exécution de leur mandat.

11.3. L'opportunité de mettre en œuvre des délais à la conservation des données à caractère personnel devrait être prise en considération lorsqu'il y a refus d'octroi d'un moyen de paiement. Des délais devraient également être établis pour tenir compte des questions telles que les besoins de garder des données durant la période nécessaire aux fins de soutien d'actions en justice ou de preuve de transactions réalisées par l'individu.

12. *Contrôle du respect des principes*

12.1. Chaque Etat devrait mettre en œuvre un mécanisme de contrôle permettant de veiller au respect des principes émis dans la présente recommandation.

12.2. A cette fin, chaque Etat devrait s'assurer que tous les organismes fournissant des moyens de paiement sont aisément identifiables.