Recommandations 02/2021 sur la base juridique pour le stockage des données relatives aux cartes de crédit dans le seul but de faciliter la poursuite des transactions en ligne

Adoptées le 19 mai 2021

Le comité européen de la protection des données

vu l'article 70, paragraphe 1, point e), du 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 (ci-après le «RGPD»),

vu l'accord EEE et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018,

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ LES RECOMMANDATIONS SUIVANTES:

1. Dans le contexte de la pandémie de COVID-19, l'économie numérique et le commerce électronique n'ont cessé de se développer. De même, les risques liés à l'utilisation des données relatives aux cartes de crédit en ligne ont augmenté. Comme l'indique le groupe de travail «Article 29» dans ses lignes directrices concernant l'analyse d'impact relative à la protection des données, les violations des données relatives aux cartes de crédit «*aurai[en]t clairement des incidences graves dans la vie quotidienne de la personne concernée*», étant donné que les données financières sont susceptibles d'être utilisées pour des «*paiements frauduleux*»[1].

2. Par conséquent, il est très important que les responsables du traitement mettent en place les garanties appropriées pour les personnes concernées et leur assurent le contrôle de leurs données à caractère personnel, afin de réduire le risque de traitement illicite et de favoriser la confiance dans l'environnement numérique. Le CEPD estime que cette confiance est essentielle à la croissance durable de l'économie numérique.

3. À cette fin, les présentes recommandations visent à encourager une application harmonisée des règles en matière de protection des données concernant le traitement des données relatives aux cartes de crédit au sein de l'Espace économique européen (EEE) et à garantir une protection homogène des droits des personnes concernées, dans le plein respect des principes fondamentaux de la protection des données requis par le RGPD.

4. Plus précisément, ces recommandations portent sur le stockage de données relatives aux cartes de crédit par les fournisseurs de biens et de services en ligne, dans le seul but précis de faciliter des achats ultérieurs par les personnes concernées[2]. Elles couvrent les cas dans lesquels une personne concernée achète un produit ou paie un service par l'intermédiaire d'un site internet ou

[1] GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES - Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679.

[2] Il convient de noter qu'elles ne concernant pas les établissements de paiement opérant dans des boutiques en ligne, ni les autorités publiques. Elles ne concernent pas non plus le stockage des données relatives aux cartes de crédit à d'autres fins, par exemple pour le respect d'une obligation légale, ou pour établir un paiement récurrent en cas de contrat à exécution successive ou d'abonnement à un service à long terme (par exemple, un contrat qui stipule la fourniture d'un certain produit chaque mois, ou l'abonnement à un service de diffusion de musique ou de films en continu).

d'une application et communique les données de sa carte de crédit, généralement sous une forme spécifique, afin de conclure cette transaction unique.

5. Comme pour tout traitement, le responsable du traitement doit pouvoir invoquer une base juridique valable en vertu de l'article 6 du RGPD pour stocker ces données. À cet égard, il convient de noter qu'un certain nombre de bases juridiques mentionnées à l'article 6 du RGPD ne seraient pas applicables à cette situation et doivent être exclues. Le stockage des données relatives aux cartes de crédit à la suite d'une transaction, afin de faciliter les achats ultérieurs, ne peut être considéré comme nécessaire au respect d'une obligation légale [article 6, paragraphe 1, point c), du RGPD] ni à la sauvegarde des intérêts vitaux d'une personne physique [article 6, paragraphe 1, point d), du RGPD]. L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement [article 6, paragraphe 1, point e), du RGPD] ne peut pas non plus être considérée comme une base juridique adéquate.

6. En outre, le stockage de données relatives aux cartes de crédit après le paiement de biens ou de services n'est pas, en tant que tel, nécessaire à l'exécution d'un contrat [article 6, paragraphe 1, point b), du RGPD]. Si, en premier lieu, le traitement des données relatives à la carte de crédit utilisée par le client pour payer est nécessaire à l'exécution du contrat, déclenchant ainsi l'application de l'article 6, paragraphe 1, point b), du RGPD, le stockage de ces données n'est utile que pour faciliter l'éventuelle prochaine transaction et faciliter les ventes. Une telle finalité ne saurait être considérée comme strictement nécessaire à l'exécution du contrat pour la fourniture du produit ou du service que la personne concernée a déjà payé[3].

7. Lorsqu'il s'agit d'un traitement nécessaire aux fins de l'intérêt légitime du responsable du traitement ou d'un tiers[4], le CEPD fait observer que pour que le responsable du traitement puisse se prévaloir de l'article 6, paragraphe 1, point f), du RGPD, les trois conditions prévues par cet article doivent être remplies[5]. Cette base juridique requiert, en premier lieu, l'identification et la qualification d'un intérêt légitime poursuivi par le responsable du traitement ou par un tiers. L'intérêt du responsable du traitement ou du tiers peut être plus large que la finalité du traitement et doit être né et actuel à la date du traitement des données[6].

8. La base juridique de l'intérêt légitime requiert, en deuxième lieu, la nécessité de traiter les données à caractère personnel aux fins de l'intérêt légitime poursuivi. En ce qui concerne cette dernière condition, pour autant que le responsable du traitement ait un intérêt légitime tel que décrit ci-dessus, il n'est pas évident que le stockage des données relatives aux cartes de crédit pour faciliter les achats ultérieurs soit nécessaire pour à la poursuite de cet intérêt légitime. En effet, la

[3] Voir également les Lignes directrices 2/2019 du CEPD sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, en particulier à la page 10.

[4] Voir l'avis 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, actuellement en cours de révision par le CEPD (voir le programme de travail 2021/2022 du CEPD adopté le 16 mars 2021).

[5] Voir arrêt de la CJUE du 4 mai 2017 dans l'affaire Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA «Rīgas satiksme», C-13/16, EU:C:2017:336, point 28.

[6] Voir arrêt de la CJUE du 11 décembre 2019 dans l'affaire TK/Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, EU:C:2019:1064, point 44.

conclusion effective d'un autre achat dépend du choix du consommateur et n'est pas déterminée par la possibilité de le réaliser «en un clic».

9. Enfin, la troisième condition requiert l'exécution d'un critère de mise en balance: l'intérêt légitime du responsable du traitement ou du tiers doit être mis en balance avec les intérêts ou les droits et libertés fondamentaux de la personne concernée, y compris les droits de la personne concernée à la protection des données et à la vie privée. Le critère de mise en balance exige de prendre en considération les circonstances particulières du traitement[7]. Un élément essentiel de l'exercice de mise en balance est l'impact potentiel du traitement sur les droits et libertés de la personne concernée[8]. Cet impact peut dépendre de la nature des données, de la méthode spécifique de traitement et de l'accès à ces données par des tiers. En ce qui concerne le critère de la nature des données, il convient de noter que les données financières ont été qualifiées par le groupe de travail «Article 29» de données à caractère hautement personnel, car leur violation a clairement des incidences graves dans la vie quotidienne de la personne concernée[9]. Par conséquent, nonobstant l'obligation du responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles de façon à garantir une sécurité appropriée des données relatives aux cartes de crédit conformément à l'article 5, paragraphe 1, point f), du RGPD et le fait que ces données peuvent être stockées à d'autres fins, leur traitement pour faciliter d'autres achats peut comporter un risque accru de violation de la sécurité des données relatives aux cartes de crédit, car il implique un traitement dans d'autres systèmes. Un autre élément important du critère de mise en balance qui pourrait être pris en considération pour évaluer l'impact du traitement sur les personnes concernées est celui des attentes raisonnables des personnes concernées sur la base de leur relation avec le responsable du traitement, du contexte et de la finalité de la collecte des données à caractère personnel[10]. Or, il apparaît qu'au moment de l'achat, tout en communiquant les données de sa carte de crédit pour réaliser le paiement, la personne concernée ne s'attend raisonnablement pas à ce que les données de sa carte de crédit soient conservées plus longtemps que ce qui est nécessaire pour payer les biens ou services qu'elle achète. Par conséquent, les droits et libertés fondamentaux de la personne concernée par la protection des données primeraient probablement sur l'intérêt du responsable du traitement dans ce contexte spécifique.

10. Ces aspects permettent de conclure que le consentement [article 6, paragraphe 1, point a), du RGPD] semble être la seule base juridique appropriée pour que le traitement décrit ci-dessus soit licite. En effet, pour faire face aux risques en matière de sécurité, pour permettre à la personne concernée de garder le contrôle de ses données et pour décider activement de l'utilisation des données relatives à ses cartes de crédit, il conviendrait d'obtenir le consentement spécifique de la personne concernée avant de stocker les données de sa carte de crédit après un achat. Ce

[7] Voir arrêt de la CJUE du 24 novembre 2011 dans les affaires jointes Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, C-468/10 et C-469/10, EU:C:2011:777, points 47 et 48; arrêt de la CJUE du 19 octobre 2016 dans l'affaire Patrick Breyer/Bundesrepublik Deutschland, C-582/14, EU:C:2016:779, point 62.
[8] Voir arrêt de la CJUE du 24 novembre 2011 précité, point 44; arrêt de la CJUE du 11 décembre 2019 précité, point 56.
[9] GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES - Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679.
[10] Voir le considérant 47 du RGPD.

consentement permettra au responsable du traitement d'attester de la volonté de la personne de faciliter ses achats ultérieurs au moyen du site web ou de l'application spécifique, ce qui ne peut être présumé par le simple fait qu'elle a conclu une ou plusieurs transactions isolées.

11. Ce consentement ne saurait être présumé: il doit être libre, spécifique, éclairé et sans ambiguïté[11]. Il doit faire l'objet d'une action affirmative claire et être demandé de manière conviviale, par exemple au moyen d'une case à cocher, qui ne doit pas être cochée au préalable[12], directement sur le formulaire utilisé pour la collecte des données. Ce consentement spécifique doit être distingué du consentement donné pour les conditions de service ou de vente et ne pas être une condition à la réalisation de la transaction.

12. Conformément à l'article 7, paragraphe 3, du RGPD, la personne concernée a le droit de retirer son consentement à tout moment quant au stockage des données relatives aux cartes de crédit afin de faciliter les achats ultérieurs. Le retrait doit être libre, simple et aussi facile pour la personne concernée qu'il lui a été facile de donner son consentement. Il doit aboutir à la suppression effective, par le responsable du traitement, des données relatives aux cartes de crédit stockées dans le seul but de faciliter les transactions ultérieures.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

[11] Voir les lignes directrices 05/2020 du CEPD sur le consentement en vertu du règlement 2016/679.
[12] *Ibidem*.