Observations du CEPD sur le projet de décision d'exécution de la Commission modifiant la décision d'exécution 2019/1765 en ce qui concerne l'échange transfrontalier de données entre les applications mobiles nationales de recherche des contacts et d'alerte dans le cadre de la lutte contre la pandémie de COVID-19

1. Introduction

Contexte du projet de proposition

- Le réseau «Santé en ligne» est un réseau constitué sur la base du volontariat qui relie les autorités chargées de la santé en ligne désignées par les États membres. Ce réseau est prévu à l'article 14 de la directive 2011/24/UE relative à l'application des droits des patients en matière de soins de santé transfrontaliers1. La décision d'exécution 2019/1765 de la Commission2 arrête les règles relatives à la création, à la gestion et au fonctionnement du réseau «Santé en ligne». L'un des principaux objectifs dudit réseau consiste, entre autres, à améliorer l'interopérabilité des systèmes nationaux de technologies de l'information et de communication et la transférabilité transfrontalière de données électroniques relatives à la santé dans le cadre de soins de santé transfrontaliers. Dans ce contexte, le réseau «Santé en ligne» et la Commission ont mis au point un outil informatique, l'infrastructure de services numériques dans le domaine de la santé en ligne (ci-après l'«eHDSI»), afin de permettre l'échange de données relatives à la santé au titre du mécanisme pour l'interconnexion en Europe[3], un programme également élaboré par la Commission. Il convient de rappeler que le CEPD et le comité européen de la protection des données (ci-après l'«EDPB») ont émis un avis conjoint 1/2019 concernant le traitement des données des patients et le rôle de la Commission européenne dans l'eHDSI[4].

- À la lumière de la crise de santé publique provoquée par la pandémie de COVID-19, les États membres de l'UE ont mis au point des applications mobiles de recherche des contacts et d'alerte. Afin d'améliorer l'interopérabilité de ces applications nationales, avec le soutien de la Commission, une infrastructure numérique a été développée par les États membres participant au réseau «Santé en ligne», lesquels ont décidé de créer un outil informatique d'échange de données, baptisé «Federation Gateway».

[1] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).
[2] Décision d'exécution (UE) 2019/1765 de la Commission du 22 octobre 2019 arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales responsables de la santé en ligne, et abrogeant la décision d'exécution 2011/890/UE (JO L 270 du 24.10.2019, p. 83).
[3] Règlement (UE) nº 1316/2013 du Parlement européen et du Conseil du 11 décembre 2013 établissant le mécanisme pour l'interconnexion en Europe, modifiant le règlement (UE) nº 913/2010 et abrogeant les règlements (CE) nº 680/2007 et (CE) nº 67/2010 (JO L 348 du 20.12.2013, p. 129).
[4] Avis conjoint 1/2019 de l'EDPB et du CEPD concernant le traitement des données des patients et le rôle de la Commission européenne dans l'infrastructure de services numériques dans le domaine de la santé en ligne (eHDSI), 15 juillet 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_opinion_201901_ehdsi_fr.pdf.

- Dans le cadre des applications de recherche des contacts, le 8 avril 2020, la Commission a adopté une recommandation concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et en sortir, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées (ci-après la «recommandation de la Commission»)5. Les États membres participant au réseau «Santé en ligne» ont adopté, avec le soutien de la Commission, une boîte à outils commune de l'UE à l'intention des États membres pour les applications mobiles en vue de soutenir la recherche des contacts[6], ainsi que des lignes directrices relatives à l'interopérabilité pour les applications mobiles de recherche des contacts approuvées dans l'UE[7]. Compte tenu de l'évolution récente de la crise de la COVID-19, la Commission[8] et l'EDPB ont publié des orientations sur les applications mobiles et les outils de recherche des contacts en ce qui concerne la protection des données et l'interopérabilité[9].

- La conception des applications mobiles des États membres et de l'infrastructure numérique permettant leur interopérabilité s'appuie sur la boîte à outils commune au niveau de l'UE, sur les orientations susvisées et sur les spécifications techniques convenues au sein du réseau «Santé en ligne». Le *Federation Gateway* vise à offrir une infrastructure informatique sécurisée fournissant une interface commune, au sein de laquelle les autorités ou les organismes officiels nationaux désignés échangeraient un ensemble minimal de données relatives aux contacts avec des personnes infectées par le SARS-CoV-2, dans le but d'informer d'autres personnes de leur exposition potentielle à cette infection et de promouvoir une coopération effective en matière de santé entre les États membres en facilitant l'échange d'informations pertinentes.

- Le projet de décision d'exécution de la Commission vise à arrêter des dispositions concernant le rôle des États membres et de la Commission dans le fonctionnement du *Federation Gateway* pour l'interopérabilité transfrontalière des applications mobiles nationales de recherche des contacts et d'alerte, tout en définissant les modalités de l'échange transfrontalier de données entre les autorités ou les organismes officiels nationaux désignés par l'intermédiaire du *Federation Gateway* au sein de l'Union.

Portée des observations

- Les présentes observations concernent le projet de décision d'exécution de la Commission modifiant la décision d'exécution 2019/1765 en ce qui concerne l'échange transfrontalier de données entre les applications mobiles nationales d'alerte et de recherche des contacts dans le cadre de la lutte contre la pandémie de COVID-19, ainsi que son annexe (qui prévoit deux annexes supplémentaires à la décision d'exécution 2019/1765).

---

[5] Recommandation (UE) 2020/518 de la Commission du 8 avril 2020 concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées.

[6] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[7] https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

[8] Communication de la Commission, Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données (JO C 124I du 17.4.2020).

[9] Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19 et la déclaration du comité européen de la protection des données du 16 juin 2020 sur les conséquences de l'interopérabilité des applications de recherche des contacts sur la protection des données, disponibles à l'adresse: https://edpb.europa.eu

- Les observations sont formulées conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725, à la suite d'une demande de consultation de la Commission européenne en date du 6 juillet 2020.

2. Observations du CEPD

2.1. Observations générales

- Le CEPD se réjouit de la décision de la Commission de définir les rôles des acteurs impliqués dans l'échange transfrontalier de données entre les applications mobiles nationales de recherche des contacts et d'alerte dans le cadre de la lutte contre la pandémie de COVID-19. Il se félicite également que le projet de décision d'exécution contienne une annexe (composée de deux annexes) qui prévoit la répartition des responsabilités entre les États membres (en tant que responsables conjoints du traitement) et la Commission (en tant que sous-traitant) pour le traitement des données à caractère personnel au sein du *Federation Gateway*. Le CEPD relève toutefois que, dans certains domaines, les annexes font essentiellement référence aux dispositions du RGPD ou les reproduisent et il est donc d'avis qu'il conviendrait de préciser davantage les choses. Sans chercher à être exhaustives, les observations suivantes contiennent un certain nombre de recommandations à cet égard.

2.2. La désignation de responsables conjoints du traitement et d'un sous-traitant

- L'article 7 bis du projet de décision d'exécution dispose que «*[l]es autorités ou organismes officiels nationaux désignés qui traitent des données à caractère personnel au sein du Federation Gateway sont les responsables conjoints du traitant des données traitées au sein dudit portail*». *D'autre part, «[l]a Commission est le sous-traitement des données à caractère personnel traitées au sein du Federation Gateway (...)*». Les responsabilités des responsables conjoints du traitement et du sous-traitant sont définies plus avant dans les annexes II et III, respectivement.

- Comme indiqué plus haut, le CEPD et l'EDPB ont déjà publié un avis conjoint sur les rôles et responsabilités des États membres et de la Commission dans le traitement des données à caractère personnel dans le cadre de l'eHDSI. Cet avis constatait que «*(...) même si elle joue un rôle dans certaines des procédures relatives à la mise en place de solutions techniques et organisationnelles ainsi qu'au niveau des éléments de sécurité des systèmes, la Commission ne jouit d'aucun pouvoir discrétionnaire sur le plan de la détermination des finalités ou des moyens essentiels de cette opération de traitement*». Dès lors, compte tenu du cadre juridique lié à la définition des finalités et des moyens de l'infrastructure, et de la stricte limitation des rôles de la Commission en vue de garantir la sécurité des services centraux de l'eHDSI, elle a été considérée comme un sous-traitant agissant pour le compte des États membres participant au réseau «Santé en ligne» lors de l'exécution du traitement des données des patients[10].

- Dans ce contexte particulier, le CEPD est d'avis que l'évaluation des rôles des parties concernées ne s'écarte pas fondamentalement de celle réalisée dans le cadre du traitement de données à caractère personnel au sein de l'eHDSI. Tant les finalités que les modalités du traitement réalisé au sein du *Federation Gateway* sont déterminées par

[10] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_opinion_201901_ehdsi_fr.pdf

le réseau «Santé en ligne»: la finalité du portail consiste à faciliter l'interopérabilité des applications mobiles nationales de recherche des contacts et d'alerte, tandis que les modalités du traitement réalisé au sein du *Federation Gateway* sont décidées par les États membres dans le cadre du réseau «Santé en ligne»[11]. La Commission émettrait à nouveau ses orientations (une fonction compatible avec celle d'un sous-traitant dans le cadre de la législation sur la protection des données) et agirait comme le fournisseur de solutions techniques et organisationnelles pour le *Federation Gateway*, en ne traitant que des données à caractère personnel anonymisées pour le compte des États membres participants.

- Le CEPD observe que l'article 7 *bis*, point 6, du projet de décision d'exécution pourrait être interprété comme limitant l'obligation de sécurité du sous-traitant à «l'hébergement et la transmission». Conformément à l'article 33 du règlement 2018/1725, le sous-traitant est tenu de garantir la sécurité de tous les traitements qu'il effectue pour le compte du responsable du traitement. Pour éviter toute ambiguïté, le CEPD recommande de remplacer les termes «de la transmission et de l'hébergement» par «du traitement, notamment la transmission et l'hébergement».

2.3. Responsabilités des responsables conjoints du traitement (annexe II)

Section 1

Sous-section 1 – Répartition des responsabilités

- L'article 26, paragraphe 1, du RGPD dispose que les responsables conjoints du traitement définissent de manière transparente, par accord entre eux, leurs obligations respectives aux fins d'assurer le respect des exigences du règlement. La détermination de leurs obligations respectives doit être réalisée par les responsables conjoints du traitement, «*notamment*» en ce qui concerne l'exercice des droits de la personne concernée et leurs obligations quant à la communication des informations visées aux articles 13 et 14, sauf si, et dans la mesure où, leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis.

- Il découle du libellé de l'article 26 que la répartition des responsabilités en matière de conformité entre les responsables conjoints du traitement ne se limite pas aux droits de la personne concernée et aux obligations quant à la communication des informations, mais devrait également couvrir d'autres obligations incombant au responsable du traitement pour garantir que l'ensemble du traitement conjoint est pleinement conforme aux dispositions du RGPD. Le CEPD se félicite de ce que plusieurs obligations supplémentaires soient déjà envisagées à l'annexe II du projet de décision d'exécution. Dans les sections suivantes, le CEPD formule un certain nombre de recommandations visant à rendre la répartition des responsabilités plus exhaustive.

[11] Voir également les spécifications techniques prévues par le réseau «Santé en ligne» (disponible à l'adresse: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0). Conformément à l'annexe II, section 1, sous-section 1, du projet de décision d'exécution, «*[l]es responsables conjoints du traitement traitent les données à caractère personnel par l'intermédiaire du* Federation Gateway *conformément aux spécifications techniques définies par le réseau "Santé en ligne"*».

- Le point 2 prévoit que «*[c]haque responsable du traitement est responsable du traitement des données à caractère personnel sur le* Federation Gateway*, conformément aux articles 5, 24 et 26 du règlement général sur la protection des données et à la directive 2002/58/CE*». En principe, le RGPD s'applique dans son intégralité à chacun des responsables conjoints du traitement. Le CEPD recommande à la Commission soit de préciser davantage les raisons pour lesquelles les articles 5, 24 et 26 du RGPD sont énumérés en particulier, soit de supprimer entièrement ce point, étant donné que le RGPD s'applique en tout état de cause aux responsables conjoints du traitement.

- Le point 5 se lit comme suit: «*Des instructions sont envoyées au sous-traitant par le point de contact de l'un des responsables conjoints du traitement, en accord avec les autres responsables conjoints du traitement*». L'annexe ne précise pas davantage comment les responsables conjoints du traitement parviennent à un accord. Le CEPD recommande de clarifier la manière dont cette décision serait prise. Si elle devait être prise par le réseau «Santé en ligne», nous recommandons d'ajouter une référence spécifique à tout document fournissant des détails sur le processus décisionnel au sein du réseau.

Sous-section 2 – Responsabilités et rôles pour le traitement des demandes et l'information des personnes concernées

- Le point 1 prévoit que chaque responsable du traitement communique aux utilisateurs de son application mobile nationale de recherche de contacts et d'alerte des informations sur le traitement de leurs données à caractère personnel au sein du *Federation Gateway* aux fins de l'interopérabilité transfrontalière des applications mobiles nationales de recherche de contacts et d'alerte, conformément aux articles 13 et 14 du règlement général sur la protection des données. Le CEPD rappelle que, au plus tard au moment où les données à caractère personnel sont obtenues par le(s) responsable(s) du traitement, la personne concernée doit recevoir des informations claires sur le traitement supplémentaire visant à garantir l'interopérabilité[12].

- Le point 2 prévoit que chaque responsable conjoint du traitement sert de point de contact pour les utilisateurs de son application mobile nationale de recherche des contacts et d'alerte. Il dispose également que si un responsable conjoint du traitement reçoit une demande d'une personne concernée, qui ne relève pas de sa responsabilité, il la transmet dans les meilleurs délais au responsable conjoint du traitement compétent.

- Le CEPD rappelle qu'en vertu de l'article 26, paragraphe 3, du RGPD, indépendamment des termes de l'accord conclu entre les responsables conjoints du traitement, la personne concernée peut exercer les droits que lui confère ledit règlement à l'égard de et contre chacun des responsables du traitement. En d'autres termes, il ne suffit pas qu'un responsable conjoint du traitement transmette simplement la demande de la personne concernée au responsable du traitement compétent. Il doit également veiller à ce qu'un suivi adéquat soit assuré.

- Pour faciliter les choses, le CEPD recommande de désigner un point de contact spécifique chargé de traiter cette demande et de veiller à ce que les personnes concernées

[12] Voir également la déclaration du comité européen de la protection des données du 16 juin 2020 sur les conséquences de l'interopérabilité des applications de recherche des contacts sur la protection des données, paragraphes 9 à 11.

en soient clairement informées[13]. Cela apporterait non seulement des informations plus claires et plus transparentes aux personnes concernées, mais cela pourrait également garantir un suivi adéquat de chaque demande[14].

2.4. Responsabilités du sous-traitant (annexe III)

- Le point 1 prévoit qu'en cas de sous-traitance, la Commission informe les responsables conjoints du traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants, ce qui donnerait aux responsables du traitement la possibilité de s'opposer conjointement à ces changements. Le CEPD recommande de préciser davantage la manière dont les responsables conjoints du traitement «s'opposeraient conjointement» dans la pratique. Si une objection conjointe devait être émise dans le cadre du réseau «Santé en ligne», nous recommandons d'ajouter une référence spécifique à tout document fournissant des détails sur le processus décisionnel au sein du réseau.

- Le point 3 a) prévoit que le traitement effectué par la Commission entraînera la suppression des données lorsque tous les serveurs dorsaux participants les ont téléchargées ou 14 jours après leur réception, la date la plus proche étant retenue. Le traitement de données à des fins d'interopérabilité devrait également permettre de définir des durées de conservation communes pour tous les États membres. Il est donc recommandé que la période totale de 14 jours soit également appliquée lorsque les données ont été téléchargées sur les serveurs dorsaux nationaux et elles ne devraient pas être conservées plus longtemps. Le CEPD recommande de clarifier ce point dans le texte de l'annexe.

- Conformément au point 5, la Commission devrait établir des procédures spécifiques pour la connexion entre les serveurs dorsaux et le *Federation Gateway*, qui incluent, notamment, «de définir les conditions permettant d'autoriser, notamment à la demande des responsables du traitement, la réalisation d'audits indépendants, y compris des inspections, et de contribuer à ces audits, ainsi que des contrôles des mesures de sécurité». À cet égard, le CEPD attire l'attention sur l'article 29, paragraphe 3, point h), du règlement (UE) 2018/1725, qui oblige le sous-traitant à permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et à contribuer à ces audits.

- Enfin, dans sa déclaration, l'EDPB souligne que «*[l]orsque les fournisseurs réfléchissent à la manière de rendre interopérables leurs applications de recherche des contacts, ils devraient, autant que possible, veiller à ce que cela n'entraîne pas une*

[13] Voir les Lignes directrices du CEPD sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement dans le cadre du règlement (UE) 2018/1725, disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_fr.pdf

[14] Une telle approche serait également conforme aux orientations de l'EDPB selon lesquelles toute solution interopérable doit faciliter l'exercice de leurs droits par les personnes concernées. Lorsque l'exercice des droits est possible, il ne devrait pas devenir plus contraignant pour les personnes concernées, lesquelles devraient savoir clairement à qui s'adresser pour exercer leurs droits. Déclaration du comité européen de la protection des données du 16 juin 2020 sur les conséquences de l'interopérabilité des applications de recherche des contacts sur la protection des données, paragraphe 16.

baisse du niveau de qualité ou de précision des données»[15]. À cet égard, le CEPD recommande d'aborder explicitement les mesures visant à préserver la qualité ou la précision des données à l'annexe III, point 3.

Bruxelles, le 9 juillet 2020

[15] Déclaration du comité européen de la protection des données du 16 juin 2020 sur les conséquences de l'interopérabilité des applications de recherche des contacts sur la protection des données, paragraphe 19.