Avis du comité (article 64)

Avis 12/2024 sur le projet de décision de l'autorité de contrôle française concernant le «Code de conduite applicable aux prestataires de services dans le domaine de la recherche clinique» soumis par l'EUCROF

Adopté le 18 juin 2024

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Table des matières

1 RÉSUMÉ DES FAITS 4

2 ÉVALUATION 4

2.1 Remarques générales 4

2.2 Concernant la réponse apportée par le code de conduite aux besoins du secteur 5

2.2.1 Présentation du secteur 5

2.2.2 Le propriétaire du code en tant qu'organisme représentatif 5

2.2.3 Champ d'application du traitement 6

2.2.4 Champ d'application territorial 7

2.3 Le code de conduite facilite l'application effective du RGPD 8

2.3.1 Le code en tant qu'outil pratique 8

2.3.2 Matrice d'exigences 9

2.3.3 Caractère contraignant du code 9

2.3.4 Concernant les garanties fournies par le code 9

2.3.5 Le code en tant qu'outil de responsabilisation 11

2.4 Concernant les mécanismes permettant de contrôler le respect d'un code 12

2.4.1 Adhésion au code 12

2.4.2 Suivi du code 13

2.4.3 Sanctions 14

2.4.4 Réexamen du code 14

3 CONCLUSIONS/RECOMMANDATIONS 15

4 OBSERVATIONS FINALES 16

Le comité européen de la protection des données

vu l'article 63, l'article 64, paragraphe 1, point b), et l'article 40 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 sur l'Espace économique européen (ci-après l'«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[1],

vu l'article 10 et l'article 22 de son règlement intérieur,

considérant ce qui suit:

(1) Les États membres, les autorités de contrôle, le comité européen de la protection des données et la Commission européenne encouragent l'élaboration de codes de conduite (ci-après le «code») destinés à contribuer à la bonne application du RGPD[2].

(2) La principale mission du comité européen de la protection des données (ci-après le «comité») est de garantir l'application cohérente du RGPD lorsqu'une autorité de contrôle (ci-après l'«autorité de contrôle») entend approuver un code de conduite concernant des activités de traitement menées dans plusieurs États membres (ci-après le «code transnational»), conformément à l'article 40, paragraphe 7, du RGPD et aux «lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement 2016/679» (ci-après les «lignes directrices»).

(3) Le comité salue les efforts consentis par les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants pour élaborer des codes de conduite qui constituent des outils pratiques et présentant potentiellement un bon rapport coût-efficacité, afin d'assurer une plus grande cohérence au sein d'un secteur donné ainsi que de favoriser le droit au respect de la vie privée et à la protection des données des personnes concernées en renforçant la transparence.

(4) Le présent avis vise à garantir l'application cohérente du RGPD, notamment par les autorités de contrôle, les responsables du traitement et les sous-traitants, ainsi qu'à mettre en évidence les éléments essentiels que doit contenir un code de conduite.

(5) Chaque code de conduite devrait faire l'objet d'un examen individuel en tenant compte des caractéristiques spécifiques du secteur concerné, sans préjudice de l'évaluation de tout autre code de conduite. Le comité rappelle que les codes sont l'occasion d'établir un ensemble de règles contribuant à la bonne application du RGPD de façon pratique, transparente et rentable, en intégrant les spécificités d'un secteur particulier et/ou de ses activités de traitement.

[1] Dans le présent avis, on entend par «États membres» les États membres de l'EEE.
[2] Article 40, paragraphe 1, du RGPD.

(6) Le comité souligne que les codes de conduite sont des outils de responsabilisation volontaires, et que l'adhésion à un code n'empêche pas les autorités de contrôle d'exercer leur pouvoir et leurs prérogatives en matière d'application des règles.

(7) Le présent code n'est pas un code de conduite au sens de l'article 46, paragraphe 2, point e), applicable aux transferts internationaux de données à caractère personnel, et il ne fournit donc pas de garanties appropriées dans le cadre des transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales dans les conditions visées à l'article 46, paragraphe 2, point e). En effet, le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si les dispositions du chapitre V du RGPD sont respectées.

(8) Conformément à l'article 64, paragraphe 3, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur du comité, l'avis du comité est adopté dans un délai de huit semaines après que le président a décidé que le dossier était complet,

A ADOPTÉ L'AVIS SUIVANT:

1 RÉSUMÉ DES FAITS

1. Conformément à la procédure de coopération définie dans les lignes directrices relatives aux codes de conduite[3], le projet de code de conduite applicable aux prestataires de services dans le domaine de la recherche clinique de l'EUCROF (ci-après le «projet de code EUCROF», le «projet de code» ou le «code») a été examiné par l'autorité de contrôle française en tant qu'autorité de contrôle compétente (ci-après l'«autorité de contrôle compétente»).
2. Le code EUCROF a été examiné dans le respect des procédures mises en place par le comité.
3. L'autorité de contrôle compétente a présenté son projet de décision concernant le projet de code EUCROF et a demandé l'avis du comité conformément à l'article 64, paragraphe 1, point b), du RGPD, le 5 février 2024. La décision relative au caractère complet du dossier a été prise le 12 mars 2024.
4. Conformément à l'article 10, paragraphe 2, du règlement intérieur du comité, en raison de la complexité du dossier, la présidente a décidé de prolonger de six semaines supplémentaires la période d'adoption initiale de huit semaines.

2 ÉVALUATION

2.1 Remarques générales

5. Le comité se félicite des références faites à l'avis du comité dans la note de bas de page 1 concernant «l'explication de la distinction entre le consentement obtenu pour la participation à la recherche clinique et le consentement obtenu pour le traitement de données à caractère personnel», aux lignes directrices du comité dans la note de bas de page 13 concernant le

[3] Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement 2016/679, adoptées par le comité européen de la protection des données le 4 juin 2019.

«champ d'application territorial du RGPD (article 3)» et aux lignes directrices du comité dans la note de bas de page 14 concernant la «notification des violations des données à caractère personnel au titre du RGPD». Toutefois, le comité constate que les liens vers le comité font défaut et recommande donc à l'autorité de contrôle française d'exiger du propriétaire du code qu'il ajoute cette référence dans les notes de bas de page pertinentes, à des fins de clarté.

2.2 Concernant la réponse apportée par le code de conduite aux besoins du secteur

2.2.1 Présentation du secteur

6. La recherche clinique correspond aux études scientifiques réalisées sur la personne humaine, en vue du développement des connaissances biologiques ou médicales. Il existe deux types d'études cliniques: les études interventionnelles (également appelées «essais cliniques») et les études observationnelles.

7. Les projets de recherche clinique sont généralement menés à l'initiative d'un promoteur (par exemple, une entreprise pharmaceutique). Pour la mise en œuvre de ces études, le promoteur peut recourir aux services d'une organisation de recherche sous contrat. Les contrats conclus entre les promoteurs de projets de recherche clinique et les organisations de recherche sous contrat précisent les services à fournir et contiennent les obligations incombant à l'organisation de recherche sous contrat en vertu de l'article 28 du RGPD.

8. Le comité note que le projet de code fait référence aux laboratoires pharmaceutiques plutôt qu'aux entreprises. Le comité encourage donc l'autorité de contrôle française à exiger du propriétaire du code qu'il remplace ce terme par le terme «entreprises» à des fins de précision.

9. Le projet de code EUCROF couvre à la fois les essais cliniques et la recherche non interventionnelle. Le code a pour objet de décrire les obligations des prestataires de services de recherche clinique, en tant que sous-traitants au sens de l'article 28 du RGPD, dans le cadre de l'exécution du contrat qui les lie au promoteur.

2.2.2 Le propriétaire du code en tant qu'organisme représentatif

10. Les codes de conduite doivent être soumis pour approbation à l'autorité de contrôle compétente, conformément à l'article 55 du RGPD. Dans le cas des codes transnationaux, lors de l'identification de l'autorité de contrôle compétente, certains facteurs peuvent être pris en compte, par exemple l'endroit où la densité de l'activité de traitement est la plus élevée ou l'endroit où le propriétaire du code a son siège[4].

11. Le propriétaire du code est la Fédération européenne des organisations de recherche sous contrat, l'«EUCROF», qui est une entité juridique sans but lucratif enregistrée aux Pays-Bas. Dans la section 1.1 du code, le propriétaire du code explique que ses objectifs sont «notamment, de contribuer à la recherche clinique sur la personne humaine et de promouvoir l'excellence de la recherche clinique européenne auprès du public et des médias, ainsi que sur la scène internationale». Les membres de l'EUCROF sont des associations nationales d'organisations de recherche sous contrat ainsi que des organisations de recherche sous contrat individuelles établies dans un ou plusieurs pays européens ou en dehors de l'Europe,

[4] Voir l'annexe 2 des lignes directrices.

telles que définies dans ses statuts. À ce jour, selon le code, l'EUCROF compte plus de 360 entreprises membres dans 25 pays, dont plus de 300 sont des PME.

12. Le propriétaire du code a identifié l'autorité de contrôle française comme l'autorité de contrôle compétente aux fins de l'approbation du code EUCROF. Le propriétaire du code a justifié son choix dans le code de conduite en se fondant sur la «proximité [de l'autorité de contrôle compétente] par rapport à l'endroit où la densité d'organisations de recherche sous contrat est la plus élevée en Europe» et sur le fait que l'autorité de contrôle française «possède une expérience considérable en matière de protection des données à caractère personnel dans les domaines des soins de santé et de la recherche clinique, étant donné qu'elle a pris des initiatives pour publier des outils et des lignes directrices afin d'aider les organisations et les entreprises à se conformer au RGPD»[5]. Le code a également souligné que le choix de l'autorité compétente «est sans préjudice des pouvoirs conférés à toutes les autorités de contrôle par le RGPD et les autorités de contrôle conservent tous les pouvoirs qui leur sont conférés en vertu de l'article 55 du RGPD»[6].

13. Conformément à l'article 40, paragraphe 2, du RGPD, un code de conduite doit être élaboré par des associations ou d'autres organismes représentant des catégories de responsables du traitement ou de sous-traitants (propriétaires du code). Le propriétaire du code ayant un rôle majeur à jouer pour assurer la cohérence et l'harmonisation des pratiques dans le secteur concerné par le code, il doit démontrer à l'autorité de contrôle compétente qu'il dispose effectivement de la qualité d'organisme représentatif. Ainsi, comme indiqué dans les lignes directrices, le propriétaire du code devrait être capable de comprendre les besoins de ses membres et de définir clairement l'activité de traitement ou le secteur auquel le code doit s'appliquer[7].

14. Le considérant 99 du RGPD recommande de consulter les parties intéressées lors de l'élaboration d'un code de conduite. La section 1.1 du code indique que le groupe de travail chargé de rédiger le code «a effectué une vaste consultation auprès des membres de l'EUCROF, ainsi que des représentants d'autres parties prenantes: l'industrie pharmaceutique, les associations de patients, les entreprises de dispositifs médicaux, les représentants des comités d'éthique, les représentants de diverses organisations universitaires, des avocats spécialisés dans les systèmes de santé électroniques ainsi que les experts en certifications ISO». Le comité note que le propriétaire du code a démontré qu'il dispose effectivement de la qualité d'organisme représentatif, capable de comprendre les besoins de ses membres.

2.2.3 Champ d'application du traitement

15. Les projets de recherche clinique sont menés à l'initiative d'un promoteur (par exemple, une entreprise pharmaceutique). Pour la mise en œuvre de ces études, le promoteur peut recourir aux services d'une organisation de recherche sous contrat. Les contrats conclus entre les promoteurs de projets de recherche clinique et les organisations de recherche sous contrat précisent les services à fournir et contiennent les obligations incombant à l'organisation de recherche sous contrat en vertu de l'article 28 du RGPD.

[5] Section 1.7 du code.
[6] Section 1.7 du code.
[7] Voir le point 22 des lignes directrices.

16. Le projet de code couvre à la fois les essais cliniques et la recherche non interventionnelle. Le code a pour objet de décrire les obligations des prestataires de services de recherche clinique, en tant que sous-traitants au sens de l'article 28 du RGPD, dans le cadre de l'exécution du contrat qui les lie au promoteur.

17. Le comité se félicite de l'explication détaillée du champ d'application de ce projet de code de conduite à la section 1.8. Dans cette section, il est mentionné qu'«une entité juridique agissant en tant que sous-traitant ultérieur pour une autre entité juridique du même groupe de sociétés agissant en tant que promoteur d'une recherche clinique (responsable du traitement des données) peut adhérer au présent code de conduite». Le comité ne comprend pas bien pourquoi le terme «sous-traitant ultérieur» est utilisé dans cette section. Par conséquent, le comité encourage l'autorité de contrôle française à exiger du propriétaire du code qu'il clarifie ce point dans le code ou qu'il remplace ce terme par le terme «sous-traitant».

18. En outre, en ce qui concerne la section 1.9.2 du projet de code relative aux «exclusions du présent code de conduite», le comité note que «[l]e présent code de conduite n'a pas pour objectif de couvrir de manière exhaustive tous les modèles contractuels susceptibles d'exister entre un promoteur et une organisation de recherche sous contrat et il n'est nullement obligatoire au titre du RGPD qu'un code de conduite couvre toutes les activités du secteur». En ce qui concerne cette partie du code et ce qui est exclu de son champ d'application, le comité encourage l'autorité de contrôle française à exiger du propriétaire du code qu'il indique plus clairement ce qui n'est pas couvert par le code, en ajoutant d'autres exemples de ce qui est exclu du code.

19. La section 1.8 du projet de code indique que le code entend couvrir toutes les activités de traitement de données associées aux services que les organisations de recherche sous contrat qui adhèrent au code fournissent aux promoteurs dans le cadre de contrats de services et lorsque les organisations de recherche sous contrat agissent en tant que sous-traitants et les promoteurs en tant que responsables du traitement.

20. L'annexe 2 du projet de code («classes de services relevant du champ d'application du code») contient une liste des types d'activités de traitement les plus courants couverts par le code, avec mention de leur finalité, des types de données à caractère personnel traitées et de la durée du traitement. Le comité souligne que la durée du traitement doit être décidée par le responsable du traitement. Par conséquent, le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il ajoute une remarque générale précisant que les informations fournies dans la section «durée du traitement» du code pour tous les services doivent être déterminées par le responsable du traitement des données.

21. Les activités de traitement «effectuées à la fois par les promoteurs et les organisations de recherche sous contrat qui ne relèvent pas de cette relation contractuelle» et les «activités de traitement effectuées par l'organisation de recherche sous contrat en tant que responsable du traitement des données de plein droit» sont exclues du champ d'application du code[8].

2.2.4 Champ d'application territorial

22. Le champ d'application du projet de code EUCROF est transnational et le code est destiné à s'appliquer dans toute l'Union européenne, conformément à l'article 40, paragraphe 7, du

[8] Section 1.8 du code.

RGPD. Le projet de code EUCROF a identifié toutes les autorités de contrôle de l'Union européenne en tant qu'autorités de contrôle concernées. Le comité note que le champ d'application du code ne couvre pas les pays de l'EEE.

23. Le comité note que l'annexe 1 du projet de code énumère les autorités de contrôle concernées. Le comité encourage l'autorité de contrôle française à exiger du propriétaire du code qu'il vérifie l'exactitude des noms et des coordonnées des autorités de contrôle.

24. Par exemple, la liste ne reflète pas la structure fédérale des autorités de contrôle allemandes indépendantes. Étant donné qu'en Allemagne, les organisations de recherche sous contrat et les promoteurs (par exemple, des entreprises privées, des universités ou des hôpitaux) relèvent généralement de la compétence des autorités de contrôle des Länder, il convient également de les mentionner et d'ajouter une référence (par exemple un lien). Une liste complète des autorités de contrôle des Länder allemands («Datenschutzaufsichtsbehörden der Länder») est disponible à l'adresse suivante: https://www.datenschutzkonferenz-online.de/datenschutzaufsichtsbehoerden.html

2.3 Le code de conduite facilite l'application effective du RGPD

25. Les lignes directrices indiquent que les codes doivent préciser les modalités d'application pratique du RGPD et refléter exactement la nature de l'activité de traitement ou du secteur. Ils doivent pouvoir présenter des améliorations claires et propres à l'industrie s'agissant du respect du droit en matière de protection des données. Un code ne doit pas se contenter de réaffirmer ce qui figure dans le RGPD. Il doit plutôt établir des règles concernant la voie à suivre afin d'appliquer le RGPD d'une façon spécifique, pratique et précise[9]. En outre, le code doit fournir des garanties suffisamment adaptées en vue d'atténuer les risques en matière de traitement des données et de droits et libertés des personnes[10].

26. Le projet de code EUCROF contient à la fois des exigences strictes spécifiant les dispositions du RGPD, mentionnées dans la section «Champ d'application du traitement» du présent avis, et les bonnes pratiques actuellement suivies par le secteur. Le projet de code EUCROF aide les organisations de recherche sous contrat à comprendre clairement quelles sont les obligations qui leur incombent en vertu du RGPD, facilite le respect des bonnes pratiques par les organisations de recherche sous contrat et améliore l'état de la technique en matière de protection des données dans le secteur[11]. En outre, il aide les promoteurs à optimiser et à simplifier le suivi du respect du RGPD par les organisations de recherche sous contrat[12].

2.3.1 Le code en tant qu'outil pratique

27. Le projet de code EUCROF clarifie ce que les exigences du RGPD signifient dans la pratique lorsqu'elles sont appliquées par les organisations de recherche sous contrat, et quelles sont les mesures concrètes que les différentes organisations de recherche sous contrat doivent prendre pour garantir le respect du RGPD. Le projet de code EUCROF décrit les droits et obligations des organisations de recherche sous contrat qui adhèrent au code sur la base des principes clés du

[9] Points 36 et 37 des lignes directrices.
[10] Point 39 des lignes directrices.
[11] Section 1.6 du code.
[12] Section 1.6 du code.

RGPD, tels que la limitation de la finalité, les droits des personnes concernées, les transferts, la sécurité, les audits, la responsabilité, etc.

2.3.2 Matrice d'exigences

28. Le projet de code consiste en un ensemble d'exigences que les organisations de recherche sous contrat doivent mettre en œuvre pour se conformer au code.

2.3.3 Caractère contraignant du code

29. Toutes les dispositions du projet de code ainsi que les objectifs et exigences de l'EUCROF en matière de sécurité sont contraignants pour les classes de services définies dans la déclaration d'applicabilité, pour lesquelles une organisation de recherche sous contrat déclare se conformer au code. Dans l'ensemble du code, les dispositions utilisent le présent et le verbe «devoir». Certaines dispositions doivent être considérées comme des orientations, donnant des exemples de bonnes pratiques, et se caractérisent par l'utilisation des termes «devrait» ou «peut».

2.3.4 Concernant les garanties fournies par le code

30. Conformément aux lignes directrices[13], un code de conduite doit fournir des garanties suffisantes tout en étant axé de façon appropriée sur les domaines et problèmes de la protection des données propres au secteur spécifique auquel il s'applique («valeur ajoutée»). Le projet de code EUCROF fournit des garanties suffisantes, par exemple en adoptant la même terminologie que celle utilisée dans le RGPD (section 1.4 du code) et en prévoyant un mécanisme de plainte pour les personnes concernées (section 5.7 du code). En ce qui concerne la valeur ajoutée, le projet de code fournit des orientations adaptées au secteur concernant, entre autres, les mesures de sécurité, les exigences en matière d'audit, les droits des personnes concernées et les exigences de transparence.

31. Le comité prend note de la section 2.2.1 du projet de code, dans laquelle il est indiqué que «sauf instruction contraire du promoteur et requise par les services/processus fournis, les organisations de recherche sous contrat ne traitent pas les données qui identifient directement le participant. Les participants aux études sont identifiés uniquement à l'aide d'un code d'identification spécifique à l'étude, ce qui constitue une pseudonymisation au sens de l'article 4, paragraphe 5, du RGPD». Le comité est d'avis que cette disposition du code n'est pas suffisante et recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il spécifie la finalité (les besoins) du processus de pseudonymisation et qu'il détermine mieux les conditions et les garanties en vertu desquelles les organisations de recherche sous contrat peuvent exceptionnellement avoir accès à l'identité du participant si nécessaire, soit à la section 2.2.1, soit à la section 3.6.3 du projet de code.

32. De même, le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il ajoute des références aux orientations et recommandations du comité sur les méthodes de pseudonymisation.

33. De même, à la section 3.6.1 du projet de code de conduite relative à la «pseudonymisation», le code indique dans la note que «l'organisation de recherche sous contrat devrait veiller à ce que

[13] Voir le point 36 des lignes directrices.

les codes prévoient des méthodes suffisamment efficaces de pseudonymisation et présentent une séquence aléatoire de symboles sans schéma facilement reconnaissable dans le cadre d'une étude, susceptible d'entraîner un risque d'identification». Le comité note que la référence à «sans schéma facilement reconnaissable» n'est pas suffisante et recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il supprime le terme «facilement», mais aussi qu'il précise que l'organisation de recherche sous contrat doit tenir compte du risque d'identification et choisir les techniques appropriées pour atténuer le risque identifié.

34. Le comité note que la section 3.2.2 du projet de code relative à l'utilisation secondaire des données à caractère personnel à des fins de recherche scientifique précise que la base juridique de ce traitement est «l'article 5, paragraphe 1, point b), et l'article 6, paragraphes 1 et 4, du RGPD». Le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il précise dans le code que l'article 5, paragraphe 1, point b), et l'article 6, paragraphe 4, du RGPD ne s'appliquent pas nécessairement de manière cumulative lorsque les opérations de traitement ultérieures poursuivent des finalités de recherche scientifique. En outre, le code devrait également faire référence à l'article 9, paragraphe 2, du RGPD lorsque le traitement concerne des catégories particulières de données à caractère personnel à des fins de recherche scientifique. Par conséquent, le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il modifie la section 3.2.2 comme indiqué.

35. Le comité note que la classe de services 17 (c'est-à-dire la fourniture d'infrastructures d'hébergement physique) est exclue de la section 3.6 relative à l'intégrité et à la confidentialité du projet de code. Le comité est d'avis que les exigences de la section 3.6 s'appliquent également à la classe de services 17 et recommande donc à l'autorité de contrôle française d'exiger du propriétaire du code qu'il modifie cette disposition du code en conséquence.

36. En ce qui concerne la mention (à la section 3.4.2.d) «Veuillez noter que, dans certains cas, par exemple, les ensembles de données d'images DICOM, des processus automatiques d'"anonymisation" peuvent être mis en œuvre au moment du téléchargement dans l'eCRF» figurant dans la section 3.4.2.1 du projet de code relative à la «collecte de données par les professionnels de la santé», le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il remplace le terme «anonymisation» par le terme «pseudonymisation», étant donné qu'il convient de comprendre qu'il s'agit de cela.

37. De même, dans la même section du projet de code et afin d'éviter toute ambiguïté, le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il précise si le terme «peuvent» fait référence à l'utilisation des outils automatiques de pseudonymisation des images.

38. À la section 3.5.f, le projet de code indique que «l'organisation de recherche sous contrat supprime ou anonymise toute donnée pour laquelle elle n'est pas en mesure d'identifier une nécessité ou une finalité déterminée. La suppression et l'anonymisation des données sont effectuées conformément aux normes sectorielles reconnues et sont vérifiées, afin de s'assurer que toutes les données à caractère personnel ont été supprimées ou écrasées de manière sécurisée». Conformément à l'article 28, paragraphe 3, point g), du RGPD, il n'appartient pas au sous-traitant (l'organisation de recherche sous contrat) de décider s'il doit anonymiser les données à caractère personnel ou les supprimer après la fin du service convenu. Conformément à l'article 28, paragraphe 3, point g), du RGPD, les données à caractère personnel doivent être supprimées ou renvoyées et les copies existantes doivent être détruites, à moins que le droit

de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel. Dans la même section du projet de code à la page 34, le troisième exemple décrit une situation dans laquelle le promoteur ordonne à l'organisation de recherche sous contrat d'enregistrer des données à caractère personnel pour son compte, par exemple à des fins d'utilisation secondaire, de sorte que ce traitement relèverait du contrat de service. La mesure 3.5.f concerne uniquement les données pour lesquelles une finalité ne peut être identifiée dans le cadre du contrat de services. Par conséquent, et afin de garantir la cohérence avec le RGPD, le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il supprime la référence à l'anonymisation des données, qu'il aligne le libellé de cette disposition du code sur l'article 28, paragraphe 3, point g), du RGPD et qu'il précise que l'organisation de recherche sous contrat agit conformément aux instructions du responsable du traitement.

39. En outre, la section 4.2 du projet de code de conduite, relative aux «mesures techniques et organisationnelles» se concentre principalement sur la mise en place et la mise à jour d'un système de gestion de la sécurité de l'information, faisant référence à la norme ISO 27001. La section 4.2 fait également référence à la norme ISO 27701 (extension de la certification ISO 27001 pour la gestion de l'information en vue de la protection de la vie privée) et le document 02 du code (matrice et exigences) énumère 12 exigences ISO 27701. Conformément à l'article 32 du RGPD, les mesures techniques et organisationnelles ne se limitent pas à la mise en place d'un système de gestion de la sécurité de l'information. Un système de gestion de la sécurité de l'information peut effectivement faire partie intégrante des mesures techniques et organisationnelles prévues par le RGPD, mais les objectifs d'un tel système et ceux de l'article 32 du RGPD diffèrent considérablement. Lorsqu'il s'agit de déterminer les mesures techniques et organisationnelles appropriées, l'article 32 du RGPD prend pour point de départ les personnes concernées et l'exercice de leurs droits fondamentaux, ce qui diffère de la perspective adoptée en matière de sécurité des technologies de l'information. Un système de gestion de la sécurité de l'information est axé sur la sécurité de l'information et vise à protéger l'institution qui traite les données et il ne suffit donc pas à garantir le respect de l'article 32 du RGPD. Compte tenu de ce qui précède, le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il précise dans le code qu'une référence à un système de gestion de la sécurité de l'information n'est pas suffisante pour garantir le respect de l'article 32 du RGPD.

2.3.5 Le code en tant qu'outil de responsabilisation

40. Les objectifs du projet de code EUCROF sont les suivants[14]:

    - définir les exigences du RGPD, en tenant compte des réglementations nationales et internationales en matière de recherche clinique applicables aux activités de traitement des données des organisations de recherche sous contrat en vigueur de temps à autre[15], et en imposant ces exigences aux organisations de recherche sous contrat qui adhèrent au code;

[14] Section 1.6 du code.

[15] Le code sera revu si de nouvelles recommandations ou lignes directrices substantielles sont publiées, en fonction de leur incidence sur toute spécificité du code. Toutefois, les généralités du code sont jugées suffisantes pour qu'une organisation de recherche sous contrat puisse se conformer aux nouvelles lignes directrices sans révision du code.

- proposer un modèle de conformité clair tant pour les petites que pour les grandes organisations de recherche sous contrat et, partant, aider celles-ci à se conformer aux règles du RGPD en leur fournissant un ensemble de bonnes pratiques et de modes opératoires adaptés au secteur de la recherche clinique;
- optimiser et simplifier le processus permettant à un promoteur de contrôler le respect du RGPD par les organisations de recherche sous contrat qui adhèrent au code;
- établir la confiance des parties prenantes (promoteurs, participants, organismes de réglementation, enquêteurs et autres membres de l'équipe de recherche clinique), en améliorant la transparence du traitement des données à caractère personnel dans le cadre de la recherche clinique;
- établir une base commune et reconnue en matière de sécurité des systèmes d'information pour la recherche clinique utilisés et/ou fournis par les organisations de recherche sous contrat, de sorte à favoriser et faciliter l'innovation, l'adoption et la bonne utilisation des nouvelles technologies dans le cadre de la recherche clinique[16];
- il convient de noter qu'une approche harmonisée à l'égard de la sécurité des systèmes d'information, fondée sur des normes déjà reconnues, ne signifie pas que les positions des États membres de l'UE sont harmonisées en ce qui concerne l'adoption de l'innovation dans des domaines d'application spécifiques (par exemple, eCRF, eConsent, eSource, rSDV, eTMF, IdO et objets connectés pour les études en situation réelle, etc.);
- fournir un modèle de gouvernance clair au niveau européen, ayant obtenu un avis favorable du comité européen de la protection des données et l'approbation de l'autorité de contrôle compétente;
- un tel modèle de gouvernance a des effets juridiques pour les organisations qui adhèrent au code et pour celles qui s'appuient sur l'adhésion des organisations de recherche sous contrat audit code, étant donné que le code peut être utilisé comme un élément permettant de démontrer le respect des exigences énoncées dans le RGPD; et
- contribuer à l'harmonisation de la mise en œuvre du RGPD dans le domaine de la recherche clinique par toutes les parties prenantes et dans l'ensemble de l'Union européenne.

41. Le comité recommande à l'autorité de contrôle française d'exiger que le propriétaire du code ajoute à l'annexe 3 et à l'annexe 4, en plus du président du comité de contrôle («COSUP»), le vice-président, à des fins d'exhaustivité, afin de couvrir toutes les fonctions au sein du COSUP.

2.4 Concernant les mécanismes permettant de contrôler le respect d'un code

42. Conformément à l'article 40, paragraphe 4, du RGPD et aux lignes directrices[17], un code doit être accompagné de la mise en œuvre de mécanismes adaptés afin de garantir que ses règles soient contrôlées de façon appropriée et que des mesures de mise en application efficientes et pertinentes soient instaurées pour en assurer la pleine conformité. Un code doit en particulier déterminer et proposer des structures et procédures prévoyant un contrôle efficace et l'application de sanctions.

2.4.1 Adhésion au code

[16] Le document de recommandation de l'EMA du 14 décembre 2022 sur les éléments décentralisés des essais cliniques donne des exemples de la relation fondamentale qui existe entre la protection des données et l'innovation dans la recherche clinique.
[17] Voir le point 40 des lignes directrices.

43. Le code doit prévoir un mécanisme d'adhésion.

44. Un mécanisme d'adhésion efficace doit définir un processus divisé en trois phases qui coïncident avec la «durée de vie» du code de conduite. Au cours de la première phase, le mécanisme doit préciser que les membres qui adhèrent au code sont tenus de respecter toutes les exigences du code, et que l'organisme de suivi évalue l'éligibilité des candidats souhaitant souscrire au code. Dans une deuxième phase, le mécanisme décrit les modalités du suivi qui est effectué de manière continue, puis de manière ponctuelle au cours de la troisième phase[18]. Le code EUCROF met au point un mécanisme d'adhésion qui respecte les trois phases du suivi.

45. En ce qui concerne le point 5 de la section 5.5.6 du projet de code relative au «niveau 2: évaluation par un tiers», le comité encourage l'autorité de contrôle française à exiger du propriétaire du code qu'il ajoute, en plus de l'«approbation ou l'approbation conditionnelle», une possibilité de refus.

46. Le projet de code prévoit deux mécanismes d'adhésion: 1. la période de procédure déclarative, au cours de laquelle l'organisation de recherche sous contrat candidate fournit la documentation (le niveau 1, la «procédure d'adhésion déclarative», décrit à la section 5.5.5 du code) et 2. la période de suivi de l'adhésion au code, prenant la forme d'un audit sur place (le niveau 2, l'«évaluation par un tiers», décrit à la section 5.5.6). Dans les deux cas, l'organisme de suivi («COSUP») valide les candidatures. La décision du COSUP déclarant qu'une organisation de recherche sous contrat adhère au code a une durée de validité de 3 ans à compter de la date de la décision. En outre, les organisations de recherche sous contrat qui adhèrent au code doivent respecter toutes les dispositions du code (pour les services), que le candidat demande une adhésion de niveau 1 ou de niveau 2. Le comité estime, en ce qui concerne le premier mécanisme d'adhésion, qu'une simple liste de contrôle fournie par le candidat souhaitant appliquer le code ne devrait pas suffire pour satisfaire aux exigences d'adhésion. En particulier, les organisations de recherche sous contrat candidates doivent fournir une documentation détaillée prouvant qu'elles respectent toutes les dispositions du code. En outre, il doit être précisé dans le code que l'organisme de suivi a le pouvoir de demander à l'organisation de recherche sous contrat candidate de fournir des documents supplémentaires si nécessaire. Le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il tienne compte de tout ce qui précède et qu'il modifie les dispositions pertinentes du code en conséquence.

2.4.2 Suivi du code

47. Le comité note qu'à la section 5.1.2 relative à la responsabilité juridique, le projet de code indique que «l'EUCROF a une responsabilité juridique en ce qui concerne le suivi du présent code de conduite et assume l'entière responsabilité pour toute violation des obligations incombant au COSUP en vertu de l'article 41, paragraphe 4, du RGPD. L'EUCROF dispose de toutes les assurances et réserves nécessaires pour couvrir les risques inhérents à ces opérations». D'abord, le comité note que cette disposition n'est pas conforme aux exigences de l'autorité de contrôle française en matière d'agrément des organismes de suivi (section 9.1.2) qui prévoient que «l'organisme de suivi reste responsable envers l'autorité de contrôle de toutes les tâches et décisions liées à ses missions», étant donné que, dans la disposition pertinente du code, la responsabilité juridique incombe entièrement au propriétaire du code (EUCROF) et non à l'organisme de suivi (COSUP). Par conséquent, le comité

[18] Point 70 des lignes directrices.

recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il modifie cette section et l'aligne sur les exigences de l'autorité française de suivi en matière d'agrément des organismes de contrôle.

48. En outre, le comité note que l'organisme de suivi (COSUP) est un organisme de suivi interne, qu'il ne s'agit pas d'une entité juridique et qu'il n'existe aucune possibilité de sanction à l'encontre du COSUP. Le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il prévoie que l'organisme de suivi reste responsable devant l'autorité de contrôle de toutes les tâches et décisions liées à ses missions et que le propriétaire du code prend les mesures nécessaires à cette fin.

    Le comité note qu'en vertu de la section 5.2.2 du projet de code, «[l]e président et le vice-président du COSUP sont élus par et parmi les membres du COSUP. Sous réserve du processus d'installation initial décrit à la section 5.2.6, ils sont élus par vote à la majorité simple par tous les membres du COSUP». Le comité comprend également qu'en vertu des règles fixées par le projet de code, au cours d'un mandat donné, le président et le vice-président élus du COSUP pourraient être tous deux des représentants d'organisations de recherche sous contrat. Afin de mieux représenter la diversité des membres du COSUP et d'éviter que les organisations de recherche sous contrat ne soient surreprésentées, le comité recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il prévoie qu'au cours d'un mandat donné, le président et le vice-président ne peuvent pas tous deux être des représentants d'organisations de recherche sous contrat.

49. Enfin, le comité rappelle que le code de conduite ne sera pas opérationnel tant que l'organisme de suivi désigné n'aura pas été agréé[19].

2.4.3 Sanctions

50. Conformément à l'article 40, paragraphe 4, du RGPD et aux lignes directrices, sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente, l'organisme de suivi désigné par le propriétaire du code prend, sous réserve de garanties appropriées, les mesures appropriées en cas de violation du code par un responsable du traitement ou un sous-traitant. Ces sanctions vont du blâme non public mais officiel, jusqu'à l'exclusion temporaire ou définitive. L'organisme de suivi s'engage à informer l'autorité de contrôle compétente de toute mesure prise en ce sens (section 5.8 du code).

51. Afin de garantir la transparence à l'égard des entités qui adhèrent au code, le code comporte une liste de mesures correctrices qui doivent être appliquées par l'organisme de suivi. À cette fin, le code EUCROF définit un cadre d'application qui détermine la sanction appropriée à appliquer par l'organisme de suivi.

2.4.4 Réexamen du code

52. Conformément à l'article 40, paragraphe 2, du RGPD et aux lignes directrices, le code prévoit un mécanisme de réexamen approprié pour garantir qu'il est toujours conforme aux normes juridiques et techniques. En particulier, la section 5.10 du code EUCROF prévoit qu'un

[19] Lorsque plusieurs organismes de suivi sont désignés par le code, l'agrément de l'un d'entre eux suffit à conférer au code de conduite un caractère contraignant.

réexamen régulier du code destiné à tenir compte des évolutions juridiques, technologiques ou opérationnelles et des bonnes pratiques a lieu lorsque nécessaire.

3 CONCLUSIONS/RECOMMANDATIONS

53. En conclusion, le comité européen de la protection des données:

1. recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il ajoute une référence au comité européen de la protection des données dans les notes de bas de page pertinentes;

2. recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il spécifie la finalité (les besoins) du processus de pseudonymisation et qu'il détermine mieux les conditions et les garanties en vertu desquelles les organisations de recherche sous contrat peuvent exceptionnellement avoir accès à l'identité du participant si nécessaire, soit à la section 2.2.1, soit à la section 3.6.3 du projet de code;

3. recommande, de même, à l'autorité de contrôle française d'exiger du propriétaire du code qu'il ajoute des références aux orientations et recommandations du comité européen de la protection des données sur les méthodes de pseudonymisation;

4. concernant la section 3.6.1 du projet de code de conduite, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il supprime le terme «facilement», mais aussi qu'il précise davantage que l'organisation de recherche sous contrat doit tenir compte du risque d'identification et choisir les techniques appropriées pour atténuer le risque identifié;

5. recommande, concernant la section 3.2.2, à l'autorité de contrôle française d'exiger du propriétaire du code qu'il précise dans le code que l'article 5, paragraphe 1, point b), et l'article 6, paragraphe 4, du RGPD ne s'appliquent pas nécessairement de manière cumulative lorsque les opérations de traitements ultérieurs poursuivent des finalités de recherche scientifique. En outre, le code devrait également faire référence à l'article 9, paragraphe 2, du RGPD lorsque le traitement concerne des catégories particulières de données à caractère personnel à des fins de recherche scientifique;

6. en ce qui concerne la classe de services 17, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il modifie le code de manière à ce que les exigences de la section 3.6 s'appliquent;

7. concernant la section 3.4.2.d, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il remplace le terme «anonymisation» par le terme «pseudonymisation»;

8. dans la même section, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il précise si le terme «peuvent» fait référence à l'utilisation des outils automatiques de pseudonymisation des images;

9. concernant la section 3.5.f, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il supprime la référence à l'anonymisation des données, qu'il aligne le libellé de cette disposition du code sur l'article 28, paragraphe 3, point g), du RGPD et

qu'il précise que l'organisation de recherche sous contrat agit conformément aux instructions du responsable du traitement;

10. concernant la section 4.2, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il précise dans le code qu'une référence à un système de gestion de la sécurité de l'information n'est pas suffisante pour garantir le respect de l'article 32 du RGPD;

11. concernant l'annexe 2, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il ajoute une remarque générale précisant que les informations fournies dans la section «durée du traitement» pour tous les services doivent être déterminées par le responsable du traitement des données;

12. concernant les annexes 3 et 4, recommande à l'autorité de contrôle française d'exiger que le propriétaire du code ajoute le vice-président en plus du président du comité de contrôle (COSUP);

13. en ce qui concerne le mécanisme d'adhésion, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il modifie les dispositions pertinentes du code de manière à ce que les organisations de recherche sous contrat candidates à l'adhésion de niveau 1 fournissent une documentation détaillée prouvant qu'elles appliquent toutes les dispositions du code de conduite, et que l'organisme de suivi a le pouvoir de demander à l'organisation de recherche sous contrat candidate de fournir des documents supplémentaires;

14. en ce qui concerne le suivi du code, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il modifie la section 5.1.2 afin qu'elle soit conforme aux exigences de l'autorité de contrôle française en matière d'agrément des organismes de suivi, qui disposent que «l'organisme de suivi reste responsable envers l'autorité de contrôle de toutes les tâches et décisions liées à ses missions»;

15. de même, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il prévoie que l'organisme de suivi reste responsable devant l'autorité de contrôle de toutes les tâches et décisions liées à ses missions et que le propriétaire du code prend les mesures nécessaires à cette fin;

16. concernant la section 5.2.2, recommande à l'autorité de contrôle française d'exiger du propriétaire du code qu'il prévoie qu'au cours d'un mandat donné, le président et le vice-président ne peuvent pas tous deux être des représentants d'organisations de recherche sous contrat.

54. Enfin, le comité rappelle également les dispositions de l'article 40, paragraphe 5, du RGPD, et réitère qu'en cas de modification ou de prorogation du code de conduite EUCROF, l'autorité de contrôle compétente doit soumettre la version modifiée au comité conformément aux procédures définies dans les lignes directrices approuvées par le comité.

4 OBSERVATIONS FINALES

55. Le présent avis est adressé à l'autorité de contrôle française et sera publié conformément à l'article 64, paragraphe 5, point b), du RGPD.

56. Conformément à l'article 64, paragraphes 7 et 8, du RGPD, l'autorité de contrôle française communique au président sa réponse au présent avis par voie électronique, dans un délai de deux semaines suivant la réception de l'avis et indique si elle maintiendra ou si elle modifiera son projet de décision. Dans le même délai, elle fournit le projet de décision modifié ou, si elle n'a pas l'intention de suivre l'avis du comité, en tout ou en partie, elle fournit les motifs pertinents pour lesquels elle n'a pas l'intention de suivre cet avis.

57. Conformément à l'article 70, paragraphe 1, point y), du RGPD, l'autorité de contrôle française communique la décision finale au comité pour inclusion dans le registre des décisions soumises au mécanisme de contrôle de la cohérence.

58. Conformément à l'article 40, paragraphe 8, du RGPD, le comité soumet cet avis à la Commission européenne.

Pour le comité européen de la protection des données
La présidente

(Anu Talus)