Règlement Général sur la Protection des Données

RGPD

01

Code de Conduite

Pour

Prestataires de service en recherche clinique

Version 1 Draft 14

20 Juillet 2024

EUCROF, Tappersweg 12T, 2031 ET, Haarlem, The Netherlands – - Numéro de TVA : NL8172.84.369.B01
www.eucrof.eu | treasurer@eucrof.eu

Table des matières

1 Introduction

Le Code de conduite RGPD de l'EUCROF pour les Prestataires de Services de la Recherche Clinique (ci-après également dénommé le "Code" ou le "Code EUCROF") définit les exigences générales que les organismes de recherche sous contrat (CRO) et plus généralement les prestataires de services de la recherche clinique, intervenant en tant que sous-traitants au titre du RGPD, s'engagent à respecter. L'EUCROF invite les CROs de toutes tailles et fournissant tous types de services à adhérer au Code. Une CRO adhérente pourra déclarer que les services qu'elle fournit et qui entrent dans le champ d'application du Code, sont conformes au Code EUCROF et cette conformité sera reconnue par une Marque de Conformité. Elle s'engage ainsi à apporter des garanties rigoureuses en matière de protection des données pour ses activités dans la Recherche Clinique.

1.1 La Fédération européenne des CROs porteur du Code de Conduite

Le présent Code de conduite est élaboré, administré et financé par la Fédération européenne des CROs (l'EUCROF), qui est désignée comme le « porteur du Code ».

L'EUCROF est une entité juridique à but non lucratif enregistrée aux Pays-Bas dont les objectifs sont, entre autres, de contribuer à une recherche clinique de haute qualité chez l'Homme, 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 de CROs ainsi que des CROs individuelles établies dans un ou plusieurs pays européens, comme défini dans ses statuts. Aujourd'hui, l'EUCROF compte plus de 460 sociétés affiliées, dans 31 pays. Plus de 300 d'entre elles répondent à la définition des PME de l'Union Européenne (UE).

Compte tenu de son rôle fédérateur, l'EUCROF intervient en vertu du principe de subsidiarité chaque fois et partout où elle est mieux à même de soutenir les intérêts de ses membres et leurs intérêts communs, en particulier à l'échelle européenne.

Les décisions de l'EUCROF sont prises par l'Assemblée Générale de ses membres. La liste des membres de l'EUCROF, ainsi que les statuts de l'EUCROF, sont publics et peuvent être téléchargés gratuitement sur le site web de l'EUCROF (www.eucrof.eu).

La gestion quotidienne et la représentation de l'EUCROF sont assurées par un bureau exécutif composé d'un groupe de dirigeants élus (président, vice-président, secrétaire, trésorier, membre du bureau exécutif). Les mandats du Bureau exécutif sont de deux ans.

Les ressources financières de l'EUCROF proviennent (a) tout d'abord des cotisations annuelles régulières versées par ses membres, (b) de lignes budgétaires complémentaires *ad hoc* alimentées par ses membres sur une base volontaire pour subventionner des initiatives stratégiques et (c) des revenus des programmes et événements de formation et d'éducation organisés par l'EUCROF.

Tous les deux ans, l'EUCROF organise la Conférence Européenne sur la Recherche Clinique.

L'EUCROF développe ses activités à travers des groupes de travail composés d'experts sélectionnés parmi les CROs affiliées et contribuant sur une base de volontariat.

Le présent Code de Conduite a été rédigé par un groupe de travail international *ad hoc*, créé à l'initiative du groupe de travail sur les nouvelles technologies. Ce groupe de travail a largement consulté les adhérents de l'EUCROF, ainsi que des représentants d'autres parties prenantes : industrie pharmaceutique, associations de patients, sociétés de dispositifs médicaux, représentants de comités d'éthique, représentants de diverses organisations académiques, juristes spécialisés dans les systèmes de santé électroniques ainsi que des experts en certifications ISO.

1.2 Documents du Code de Conduite

La présente version du Code a été élaborée en tenant compte de la règlementation applicable en matière de protection des données à caractère personnel, et des réglementations spécifiques au domaine de la recherche clinique, en vigueur au moment de la rédaction du présent document. Ceci étant précisé, le Code n'est pas destiné à contenir les dispositions qui peuvent être prévues par la législation et les réglementations nationales spécifiques au secteur, concernant la protection des données à caractère

personnel de tous les pays dans lesquels la CRO adhérente peut être située. Les CROs qui adhèrent au Code doivent aider les promoteurs à déterminer les exigences applicables en matière de protection des données à caractère personnel en tenant compte des lois relatives à la recherche clinique.

Le présent Code de Conduite comprend les deux (2) documents suivants :

- Le document « 01 » est le présent document intitulé « Code de Conduite EUCROF pour les Prestataires de Services de la Recherche Clinique », y compris ses annexes. Il s'agit du document « maître » qui spécifie toutes les caractéristiques principales du Code.

  Les « notes » figurant dans le présent document sont destinées à fournir un deuxième niveau de lecture et des clarifications supplémentaires sur le texte principal. Les notes sont considérées comme ayant la même valeur contraignante que le texte principal.

- Le document « 02 » ; intitulé « Objectifs et exigences de sécurité ». Ce document est disponible en format PDF et XLS.

Ces deux documents ne peuvent être considérés que conjointement : aucun de ces documents pris isolément ne peut être considéré comme constituant le Code.

Pour plus de détails sur la structure de ce Code et sur la manière dont les CROs qui y adhèrent peuvent s'y conformer, veuillez vous référer à la section 1.10 ci-après.

L'EUCROF a publié un certain nombre de documents complémentaires. Ces documents **ne font pas partie** du Code et n'ont pas été approuvés par les Autorités Européennes de contrôle de la protection des données. Ils constituent une « boîte à outils » avec des modèles de documents et des guides destinés à faciliter la mise en œuvre du Code par les candidats adhérents. L'utilisation de ces outils n'est ni normative ni obligatoire. Cela signifie que les CROs peuvent utiliser toute ou une partie des outils selon leur propre choix.

Remarque :

Les exigences du Code sont identifiées par une référence unique qui renvoie à son chapitre et à sa section (par exemple, l'une des premières exigences est 2.4.a) et sont présentées dans un encadré.

1.3 Glossaire

COSUP	Comité de Supervision (Organe de gouvernance du Code)
CRF	Cahier d'Observations (voir aussi eCRF pour le Cahier d'Observations électronique)
CRO	Organisme de recherche sous contrat (Contract Research Organization)
DPA	Data Processing Agreement (Contrat pour le Traitement des Données).
EDC	Capture électronique des données (Electronic Data Capture)
CEPD	Comité Européen de la Protection des Données
EEE	Espace Economique Européen
UE	Union Européenne
EUCROF	Fédération Européenne des CROs (European CRO Federation)
RGPD	Règlement Général de Protection des Données
ICF	Formulaire de consentement éclairé (ICF – Informed Consent Form), également connu sous le nom de fiche d'information du patient[1]
PRO	Patient Reported Outcome - Résultat Rapporté par les Patients (voir aussi ePRO pour electronic Patient Reported Outcome)

[1] Voir l'avis 3/2019 du CEPD concernant les questions et réponses sur l'interaction entre le règlement sur les essais cliniques (CTR) et le règlement général sur la protection des données (RGPD) pour l'explication de la distinction entre le consentement obtenu pour la participation à la recherche clinique et le consentement obtenu pour le traitement des données à caractère personnel.

PME	Petites et moyennes entreprises
TMF	Dossier Principal de l'Essai clinique (Trial Master File). Voir aussi eTMF qui signifie electronic Trial Master File – Dossier électronique Principal de l'Essai clinique.

1.4 Terminologie, définitions

(1) Informations anonymes

Conformément au considérant 26 du RGPD, les informations anonymes sont des informations qui ne se rapportent pas à une personne physique identifiée ou identifiable ou à des données à caractère personnel rendues anonymes de telle manière que la personne concernée n'est pas ou plus identifiable. Les informations anonymes ne sont pas soumises aux exigences du RGPD.

(2) Règlementation applicable

Dans le présent document, les termes de réglementation applicable font référence au RGPD et à toute loi nationale de l'UE applicable à la protection des données à caractère personnel et mettant en œuvre le RGPD, les règlements de l'UE spécifiques au domaine de la recherche clinique et les normes technologiques régissant le traitement des données à caractère personnel de santé dans les systèmes informatisés.

(3) Étude Clinique et Recherche Clinique (également juste Etude ou Recherche)

Une Étude Clinique est une étude de recherche impliquant des volontaires humains (également appelés Sujets de l'Etude) qui a pour but d'enrichir les connaissances médicales, réalisée dans le cadre de la réglementation applicable telle que, notamment, le Règlement n°536/2014 relatif aux essais cliniques et le Règlement n° 745/2017 relatif aux dispositifs médicaux. Le terme Recherche Clinique fait référence aux études cliniques en général.

Il existe deux types d'études cliniques : les études interventionnelles (également appelées essais cliniques) et les études observationnelles.

Une étude interventionnelle est un type d'étude clinique dans laquelle les sujets de l'étude sont répartis dans des groupes qui reçoivent une ou plusieurs interventions/traitements (ou aucune intervention dans le cas d'un groupe témoin) afin que les chercheurs puissent évaluer les effets des interventions sur la santé. Les répartitions sont déterminées par le protocole de l'étude. Les sujets de l'étude peuvent recevoir des interventions diagnostiques, thérapeutiques ou autres.

Une étude observationnelle est un type d'étude clinique dans laquelle les sujets sont identifiés comme appartenant à un même groupe d'étude et dont les données de santé font l'objet d'études à des fins de recherche. Les sujets peuvent recevoir des interventions diagnostiques, thérapeutiques ou autres, mais l'investigateur n'assigne pas les sujets d'étude à une intervention ou à un traitement spécifique. Un registre de patients est un type d'étude observationnelle.

Dans le cadre du présent Code de Conduite, le terme « recherche clinique » doit être considéré dans son sens le plus large, y compris les études interventionnelles et d'observation, les études en vie réelle et tous les types d'études avec utilisation secondaire des données des patients, qu'elles soient collectées au moyen de supports papier ou électroniques, y compris les cahiers d'observations électroniques (eCRF), les résultats rapportés par les patients par voie électronique (ePRO) ou les évaluations des résultats cliniques par voie électronique (eCOA). La recherche clinique est soumise à des réglementations internationales, européennes et nationales.

(4) Données de l'étude clinique

Toutes les données collectées aux fins d'une Etude Clinique, y compris les données des professionnels de santé et des sujets de l'étude. Ces données peuvent inclure des données à caractère personnel conformément à l'article 4(1) du RGPD ainsi que des données de santé qui sont qualifiés comme des catégories particulières de données à caractère personnel conformément à l'article 9 du RGPD.

(5) COSUP (Comité de Supervision)

Organe interne de la Fédération Européenne des CROs (EUCROF), accrédité par l'autorité de contrôle compétente spécifiée au point 1.7 ci-après, doté des exigences requises pour contrôler la mise en œuvre effective du présent Code de Conduite.

(6) CRO - Contract Research Organisation (Organisation de recherche sous contrat)

Une organisation de recherche sous contrat (CRO) est une personne physique ou morale (commerciale, académique ou à but non lucratif) qui fournit des services aux Promoteurs et à d'autres parties prenantes, telles que des organisations gouvernementales, des fondations ou des hôpitaux, sur la base d'un contrat et dans le cadre de la recherche clinique (interventionnelle ou observationnelle) ou effectue d'autres activités dans des domaines connexes.

Notes :

- Cette définition a été créée et approuvée par l'EUCROF en 2017 et a été intégrée dans la dernière version du Code de Conduite pour l'indépendance scientifique et la transparence dans la conduite des études de pharmaco-épidémiologie et de pharmacovigilance approuvé par le groupe de pilotage ENCeP/ EMA.
- Cette définition concerne tous les types de « Prestataires de services » dans le domaine de la recherche clinique. Elle inclut notamment les fournisseurs de solutions informatiques, tels que les fournisseurs de systèmes de saisie électronique des données (EDC) et les fournisseurs de tous les types de systèmes d'information dédiés à la recherche clinique qui doivent se conformer, ou fournir des fonctions de conformité, aux réglementations et orientations spécifiques du secteur.
- Les CROs sont invitées à tenir compte de la définition du sous-traitant des données à l'article 4, paragraphe 8 du RGPD en ce qui concerne leur rôle dans le traitement des Données à caractère personnel pour la recherche clinique, en particulier le fait que le sous-traitant des données traite les données à caractère personnel pour le compte du responsable du traitement des données.
- Si une CRO a le statut de Site Investigateur, les services et activités de cette CRO liés à ce statut sont explicitement exclus du champ d'application du présent Code.
- Le personnel de la CRO peut fournir des services qui devraient être effectués sur le Site Investigateur, physiquement ou à distance. Ces activités/tâches sont normalement exigées dans le cadre de la sélection du site (initiation), de la surveillance du site, de l'audit sur site, des réunions investigateur/équipe du site, des services directs aux patients, etc. (voir l'annexe 2 Catégories de services relevant du présent code). Une CRO agit à tout moment au nom du promoteur, avec son autorisation et selon ses instructions, mais les tâches sont exécutées sous la supervision quotidienne du Site Investigateur.
    - Exemple

      Une CRO fournit des services de gestion du site Investigateur au Promoteur et met à disposition du personnel détaché, qui travaille directement sur le Site Investigateur, effectuant des activités pour la Recherche Clinique normalement réalisées par les membres de l'équipe investigatrice, par exemple, le coordinateur de l'étude. Le personnel est placé sous le contrôle quotidien du Site Investigateur et peut utiliser de multiples systèmes d'information du Site Investigateur et de la CRO, ou uniquement les systèmes du Site Investigateur. Le personnel détaché est employé par la CRO, et non par le Site Investigateur, et fournit un service au Promoteur. Par conséquent, la CRO n'est pas considérée comme ayant le statut de Site Investigateur, mais comme un prestataire de services agissant sous la direction du Promoteur.

Dans le présent Code de Conduite, les termes "Prestataires de services" et "CRO" sont considérés comme parfaitement équivalents. Par souci de simplicité, le terme "CRO" sera utilisé dans toutes les sections suivantes du présent Code de Conduite et sera compris comme signifiant Prestataires de Services pour la Recherche Clinique.

(7) Marque de conformité au code EUCROF

Il s'agit du badge ou de la marque qu'une CRO peut afficher une fois qu'elle a reçu l'approbation du COSUP en tant que CRO adhérant à ce Code.

(8) Exportateur

Les exportateurs désignent les commanditaires ou les prestataires de services (CRO ou sous-traitants) participant à un transfert international de données à caractère personnel en tant que cédants de données à caractère personnel.

(9) Professionnels de santé (PdS)

Dans le contexte du présent Code, également appelés membres de l'équipe d'investigation, les PdS sont des personnes physiques qui collectent des données, dirigent ou supervisent la réalisation d'une étude clinique. Les médecins agissant en tant qu'investigateurs, investigateurs principaux, investigateurs secondaires, investigateurs coordinateurs, ainsi que le coordinateur de l'étude, les investigateurs secondaires, les administrateurs de données sur site, les pharmaciens, les infirmières de l'étude, les techniciens de laboratoire et les autres membres de l'équipe de l'étude clinique agissant sous la responsabilité de l'investigateur sont des exemples de ces professionnels de la santé. La responsabilité première des professionnels de santé est de fournir des soins aux patients et, par conséquent, en tant que membres de l'équipe élargie de professionnels de santé, ils agissent en tant que responsables du traitement des données pour leurs activités de traitement liées aux soins médicaux. Dans le cadre des activités de traitement liées à l'étude clinique, les prestataires de soins de santé concernés collectent les données de l'étude clinique des sujets de l'étude, conformément aux exigences de la finalité de l'étude clinique et au protocole. Ils sont également des personnes concernées pour la CRO et/ou les promoteurs, car ces entités doivent traiter leurs données à caractère personnel pour mener à bien l'Étude Clinique.

(10) Importateur

Les importateurs désignent les commanditaires ou les prestataires de services (CRO ou sous-traitants) qui participent à un transfert international de données à caractère personnel en tant que destinataires des données à caractère personnel.

(11) Transfert international

Par transfert international de données à caractère personnel, on entend l'envoi ou la transmission de données à caractère personnel à des destinataires situés dans des pays tiers par tout moyen (y compris, mais sans s'y limiter, par courrier postal ou électronique) ou en rendant de toute autre manière les données à caractère personnel effectivement accessibles à des destinataires situés dans des pays tiers (par exemple, en téléchargeant des données à caractère personnel par voie électronique dans une base de données à laquelle des personnes situées dans des pays tiers auront effectivement accès, ou en leur accordant un accès à distance à une base de données située dans l'Union européenne).

(12) Site Investigateur ou Site de l'Investigateur

Un Site Investigateur est un prestataire de soins de santé, public ou privé, qui participe à une étude clinique dans le cadre d'un contrat avec le promoteur de l'étude.

(13) Investigateur

Chercheur participant à une étude clinique. Les termes apparentés comprennent l'investigateur principal du site, le co-investigateur du site, le Président de l'étude, le directeur de l'étude et l'investigateur principal de l'étude.

(14) Données à caractère personnel

Conformément à l'article 4(1) du RGPD, les données à caractère personnel désignent toute information se rapportant à une personne physique identifiée ou identifiable ("personne concernée") ; est "identifiable", une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.

Dans le présent code, les données à caractère personnel sont des données relatives aux personnes concernées par les études cliniques, principalement les professionnels de santé et les sujets de l'étude, ainsi que le personnel de la CRO et du promoteur, dans la mesure où elles sont utilisées dans le contexte et aux fins de l'étude clinique.

(15) Utilisation principale des données de l'étude clinique

Toutes les opérations de traitement liées à un protocole d'étude clinique spécifique pendant tout son cycle de vie, depuis le début de l'étude jusqu'à la suppression à la fin de la période d'archivage, y compris la

soumission de données dans le cadre d'autorisations de mise sur le marché ou de décisions de remboursement.

(16) Pseudonymisation

Conformément à l'article 4, paragraphe 5, du RGPD, la pseudonymisation désigne le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise, sans avoir recours à des informations supplémentaires, et à condition que ces dernières soient conservées séparément et soumises à des mesures techniques et organisationnelles visant à garantir que les Données à caractère Personnel ne puissent être attribuées à une personne physique identifiée ou identifiable.

Conformément aux articles 25(1) et 89(1) du RGPD, l'application de la pseudonymisation aux données à caractère personnel peut réduire les risques de réidentification des personnes concernées et aider les responsables du traitement et les sous-traitants à respecter leurs obligations en matière de protection des données.

(17) Utilisation secondaire des données de l'étude clinique

Dans le cadre du Code, cela signifie le traitement ultérieur, à des fins de recherche scientifique, des données de l'étude clinique dans un but autre que celui décrit par le protocole, qui est considéré comme l'utilisation principale des données de l'étude clinique. La Collecte de données supplémentaires qui peut avoir lieu dans le cadre de l'extension du même protocole, par exemple à la suite d'un amendement au protocole, n'est pas considérée comme une utilisation secondaire des données de l'étude clinique.

(18) Promoteur

Un Promoteur est l'entité juridique qui prend la responsabilité de l'initiation, de la gestion et/ou du financement d'une Étude Clinique. C'est l'entité juridique qui définit la finalité et les moyens d'une Étude Clinique et agit donc en tant que responsable du traitement conformément à l'article 4, paragraphe 7, du RGPD.

Exemples :

- Un Promoteur peut être une entreprise privée (laboratoire pharmaceutique, fabricant de dispositifs médicaux, société de biotechnologie, hôpital ou clinique privé) ou une institution académique (organisme/institution de recherche publique, hôpital public, association ou fondation médicale à but non-lucratif).

Remarque :

- Dans le contexte du présent Code, un Promoteur peut lui-même être partie à une relation de responsable du traitement conjoint avec un autre responsable du traitement, tel qu'un second Promoteur. Dans ce cas, les dispositions du présent Code peuvent toujours s'appliquer au traitement effectué par la CRO agissant en tant que sous-traitant des données pour le(s) responsable(s) du traitement. Le contrat relatif au traitement des données précise la répartition des rôles et responsabilités du responsable du traitement entre les responsables conjoints du traitement vis-à-vis de la CRO. Par exemple, il se peut qu'un seul des responsables du traitement passe un contrat avec la CRO et lui donne des instructions. Les responsables conjoints du traitement peuvent également passer ensemble un contrat avec la CRO et lui donner des instructions.

(19) Sujet d'étude

Une personne humaine qui s'est portée volontaire pour participer à une Étude Clinique dont les données à caractère personnel sont traitées par les CROs et les Promoteurs, et qui est une personne concernée conformément à l'article 4(1) du RGPD ; "*une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, (...)*". Le terme Sujet d'étude couvre également les personnes humaines autres que les Professionnels de santé dont les données peuvent être collectées dans le cadre d'une Étude clinique, telles que la partenaire enceinte, le nouveau-né ou d'autres membres de la famille agissant en tant que soignants.

(20) Pays tiers

Tout pays situé en dehors de l'Union européenne (UE) et de l'Espace économique européen (EEE).

1.5 Justification, besoin

Un Code de Conduite dédié aux CROs se justifie pour les raisons suivantes :

- Les CROs participent au traitement des données à caractère personnel dans le cadre de la Recherche clinique à tout moment en tant que Sous-traitants, depuis la phase de conception de la Recherche clinique jusqu'à la phase d'archivage ;
- Les CROs effectuent des opérations de traitement sur de grands volumes de données à caractère personnel avec des logiciels spécifiques dédiés à la Recherche clinique, y compris le traitement de catégories particulières de données au sens de l'article 9 du RGPD ;
- Les CROs jouent un rôle central entre les différents acteurs impliqués dans la recherche clinique et notamment entre les promoteurs, les Sites Investigateurs et les autorités de contrôle ; et
- Un nombre considérable de CROs sont des micro, petites et moyennes entreprises, dont les ressources pourraient être insuffisantes pour effectuer leur propre analyse de l'application du RGPD à leurs activités de traitement de données dans le secteur de la recherche clinique.

L'identification d'un manque évident d'approches harmonisées dans la mise en œuvre des exigences du RGPD lors des traitements de données dans lesquels les CROs sont impliquées est à l'origine de l'élaboration du Code.

Inviter les CROs à se conformer aux exigences établies par le Code apporte de meilleures garanties aux personnes concernées dans le cadre de la recherche clinique. Un Code de conduite contribue à la transparence des pratiques employées par les CROs et offre également une meilleure protection des données à caractère personnel, si les CROs adhérentes mettent en œuvre les principes du RGPD. L'efficacité du Code est garantie par la surveillance continue exercée par l'organisme de contrôle dédié au Code, accrédité par l'autorité principale de contrôle du Code qui a approuvé la publication du Code.

La pertinence d'un code pour les CROs a été examinée lors de discussions avec des experts en matière de protection de la vie privée et des experts cliniques, confirmée et reconnue par les autorités, notamment par un représentant de l'EDPS (European Data Protection Supervisor). La recherche clinique est mentionnée à deux reprises dans les lignes directrices 1/2019 du CEPD sur les codes de conduite et les organismes de contrôle, comme un domaine dans lequel l'élaboration d'un Code de Conduite apparait bénéfique.

Plusieurs problèmes essentiels pour les CROs ont été identifiés :

1) L'article 32 exige que les sous-traitants mettent en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque. Les CROs appliquent leur propre évaluation, ce qui entraîne des incohérences dans l'estimation des risques. L'évaluation des risques n'est pas entièrement objective. Par expérience, elle varie selon que la CRO est un prestataire de services unique ou global, selon le type de services qu'il fournit et selon qu'il n'a qu'une portée locale ou mondiale. Par conséquent, différentes organisations ont évalué très différemment le risque lié à des activités essentiellement similaires dans un contexte similaire.

   La certification ISO est une méthode fiable pour normaliser l'évaluation des mesures appropriées. L'obtention d'une certification ISO n'est souvent pas possible et/ou appropriée, en particulier pour les PME et les entreprises en phase de démarrage. Le Code fournit aux CROs un outil pratique leur permettant de définir les services, le contexte du traitement des données, le risque associé, et de lier ces facteurs aux mesures techniques qui sont nécessaires pour gérer les risques de manière cohérente, en s'appuyant sur le consensus développé par les experts du secteur. Cela permettra d'harmoniser et de renforcer le niveau minimal obligatoire de protection des données à caractère personnel offert par les organisations adhérentes.

2) L'article 28 exige que les responsables du traitement ne fassent appel qu'à des sous-traitants offrant des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées. Cette exigence expose les sous-traitants à des évaluations répétitives et hétérogènes de la part de différents clients (responsables du traitement). En raison de l'absence d'une norme sectorielle convenue concernant les mesures de sécurité appropriées dans le domaine de la recherche clinique, les responsables du traitement (promoteurs) appliquent diverses matrices internes, élaborées sur la base de leur évaluation interne des risques commerciaux et de leurs attentes à l'égard des CROs. En règle générale, les promoteurs n'acceptent pas les déclarations de conformité au RGPD élaborées par une CRO et exigent plutôt que les CROs soient évaluées selon leurs propres normes.

Avec une telle approche non harmonisée de la part des promoteurs, les CROs n'ont pas la possibilité de normaliser leurs propres processus internes. Le code EUCROF contribue à résoudre ces problèmes et les entreprises pourront mieux se concentrer sur la mise en œuvre et l'amélioration cohérentes et proportionnées des mesures. L'article 28, paragraphe 5, du RGPD précise que l'adhésion à un code peut être considérée comme offrant des garanties suffisantes. Une CRO qui a obtenu une marque de conformité au code EUCROF peut l'utiliser comme preuve de conformité reconnue par les autorités de contrôle sans avoir à remplir de nombreux questionnaires. Les ressources ainsi économisées par les responsables du traitement et les sous-traitants peuvent être investies dans une meilleure conformité ou dans le contrôle de la conformité.

3) Les CROs font appel à leur propre jugement pour élaborer des processus qui leur permettent d'atteindre et de démontrer leur conformité au RGPD. Toutefois, indépendamment de ces efforts de mise en conformité, les autorités de contrôle peuvent appliquer des sanctions à ces CROs s'il s'avère qu'elles n'ont pas respecté le RGPD, par exemple, lors d'une inspection d'une autorité de contrôle, etc. Toutefois, si la CRO adhère à un Code de Conduite, les autorités de contrôle en tiendront compte dans leur décision d'imposer ou non une amende administrative et d'en fixer le montant, conformément à l'article 83, paragraphe 2, point j), du RGPD. Cela peut signifier que les CROs qui n'ont pas cherché à se conformer à ce Code peuvent subir un préjudice financier par rapport aux adhérents au Code, ce qui constitue une bonne raison pour les CROs à adhérer au Code.

   Le Code EUCROF offre un mécanisme clair d'adhésion et de vérification connexe et fonctionne comme un livre de règles pour les sous-traitants qui conçoivent et mettent en œuvre des activités de traitement des données conformes au RGPD, ce qui est conforme aux lignes directrices 1/2019. Au fur et à mesure que le Code gagnera en importance et en reconnaissance dans le secteur, on peut s'attendre à ce que les CROs y adhèrent. Par conséquent le niveau général de conformité dans le secteur s'améliorera au rythme des sollicitations de mise en conformité.

Le présent Code prévoit des procédures et des mécanismes opérationnels standardisés pour faciliter la conformité des CROs aux exigences du RGPD en tenant compte des caractéristiques spécifiques du traitement effectué dans le secteur de la recherche clinique et, en particulier, des besoins des micro, petites et moyennes CROs.

1.6 Objet

Afin de répondre aux besoins identifiés, ce Code de Conduite vise à :

- Définir les exigences de conformité au RGPD, en tenant compte des réglementations nationales et internationales en matière de recherche clinique, applicables aux activités de traitement des données des CROs[2], et imposer ces exigences aux CROs adhérentes ;
- Proposer un modèle de Conformité clair pour les petites et grandes CROs et aider ainsi les CROs à être en conformité avec les règles du RGPD en leur apportant un ensemble de bonnes pratiques et de modes opératoires adaptés à l'industrie de la Recherche Clinique ;
- Optimiser et simplifier le processus permettant à un promoteur de contrôler la conformité au RGPD des CROs adhérentes ;
- Renforcer la confiance en améliorant la transparence du traitement des données à caractère personnel dans la recherche clinique pour les parties prenantes (promoteurs, sujets des études, organismes régulateurs, investigateurs et autres membres de l'équipe de 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 CROs, et ainsi favoriser et faciliter l'innovation, l'adoption et l'utilisation correcte des nouvelles technologies au sein de la recherche clinique[3] ;

  Il convient néanmoins de noter qu'une approche harmonisée de la sécurité des systèmes d'information, basée sur des normes déjà reconnues, ne signifie pas qu'il y a une harmonisation des positions des États

[2] Le code sera révisé si de nouvelles recommandations ou lignes directrices substantielles sont publiées, en fonction de leur impact sur le code. Toutefois, les dispositions générales du code sont considérées comme suffisantes pour qu'une CRO puisse se conformer aux nouvelles lignes directrices sans révision du code.

[3] Des exemples du lien central entre la protection des données et l'innovation dans la recherche clinique sont disponibles dans le document de recommandation de l'EMA sur les éléments décentralisés pour les essais cliniques du 14 décembre 2022.

membres de l'UE concernant l'adoption d'innovations dans des domaines d'application spécifiques (par exemple, eCRF, eConsent, eSource, rSDV, eTMF, IoT et objets connectés pour les études en vie réelle, etc.) ;

- Fournir un modèle de gouvernance clair à l'échelle européenne, ayant reçu un avis favorable du Comité Européen de la Protection des Données et l'approbation de l'autorité de contrôle compétente.
- Ce modèle de gouvernance a la valeur d'une règlementation pour les organisations qui adhèrent au Code et pour les organisations qui ont recours aux services des CROs en raison de leur adhésion au Code, du fait des garanties que cette adhésion apporte quant à la conformité au RGPD ; et
- Contribuer à l'harmonisation de la mise en œuvre du RGPD dans la recherche clinique par toutes les parties prenantes et dans l'ensemble de l'Union Européenne.

Le Code de Conduite est ainsi élaboré pour concilier la protection de la vie privée des Personnes participant à la Recherche Clinique avec la conduite de cette recherche par les CROs et la libre circulation des données indispensables à la poursuite de ces activités et au développement économique qui y est associé.

1.7 Autorité de contrôle compétente

L'autorité de contrôle identifiée comme l'autorité de contrôle compétente pour gérer la procédure de soumission du présent Code de Conduite et pour le contrôle de l'efficacité de la mise en œuvre du présent Code de Conduite est la CNIL (Commission Nationale de l'Informatique et des Libertés).

La CNIL a été considérée comme l'autorité la plus appropriée et la plus adaptée pour ce rôle, compte tenu de la forte densité de CROs présentes sur le territoire Français et du fait que la CNIL possède une expérience importante en matière de protection des données à caractère personnel dans le domaine des soins de santé et de la recherche clinique, ayant à son actif la publication d'outils et de lignes directrices pour aider les organisations et les entreprises à se conformer au RGPD.

Même si la CNIL a été l'autorité compétente pour gérer la procédure de demande de soumission du code, cela est sans préjudice des pouvoirs conférés à toutes les autorités de contrôle par le RGPD, en vertu de l'article 55 du RGPD.

1.8 Champ d'application

Ce Code de Conduite est un code transnational qui couvre les activités de traitement effectuées dans tous les États membres de l'Union européenne par les CROs qui adhèrent à ce Code.

L'annexe 1 dresse la liste de toutes les autorités de contrôle de protection des données à caractère personnel qui sont concernées.

Le présent code couvre toutes les activités de traitement des données associées aux services que les CROs adhérentes fournissent aux promoteurs dans le cadre de contrats de service et lorsque les CROs agissent en tant que sous-traitants et les promoteurs en tant que responsables du traitement.

Sans préjudice des responsabilités des parties concernées de remplir leurs obligations particulières en rapport avec le RGPD, les activités suivantes sont exclues du champ d'application du présent Code ; (a) toutes les activités de traitement menées à la fois par les promoteurs et les CROs qui ne relèvent pas de cette relation contractuelle, et (b) les activités de traitement menées par la CRO en tant que responsable du traitement des données à part entière.

Les types de services entrant dans le champ d'application du présent code sont décrits et énumérés à l'annexe 2.

Remarque :

- Les descriptions des services de l'annexe 2 ont une valeur générique; elles sont également désignées ci-après par l'expression "classes de services".

Ces services peuvent concerner tout type d'études cliniques telles que définies à la section 1.4 (3) du présent code, y compris les études interventionnelles et observationnelles, ainsi que l'utilisation primaire et secondaire des données de l'étude clinique telles que définies à la section 1.4 (15-17).

Les données à caractère personnel visées par le présent code incluent les données à caractère personnel des sujets d'étude et des professionnels de la santé traitées dans le cadre des services fournis par les CROs

aux promoteurs.

Les données à caractère personnel du personnel de la CRO et du promoteur ne sont prises en compte dans le présent Code de Conduite, que dans la mesure où elles sont utilisées dans le contexte et aux fins de la recherche clinique. Les autres finalités de traitement, par exemple l'administration générale du personnel, relèvent de la responsabilité distincte de chaque partie et n'entrent pas dans le champ d'application du présent Code de Conduite.

Notes :

- Une entité juridique agissant en tant que sous-traitant pour le compte d'une autre entité du même groupe de sociétés agissant en tant que promoteur d'une recherche clinique (responsable du traitement) peut adhérer au présent Code de Conduite.
- Une CRO non établie dans l'Union européenne est éligible à l'adhésion au présent Code dans la mesure où les activités de traitement couvertes par le Code sont soumises au RGPD en vertu de l'article 3, paragraphe 2, cette CRO devant démontrer sa conformité aux exigences du chapitre V du RGPD et de la section 4.6 du présent Code.
- Une personne morale répondant à la définition de CRO qui n'est pas membre de l'EUCROF est éligible à l'adhésion au présent Code de Conduite et les frais payés pour l'adhésion ne confèrent pas la qualité de membre d'EUCROF.
- Le présent Code de Conduite ne vise pas nécessairement à couvrir tous les processus potentiels qui pourraient être mis en œuvre dans le cadre d'un projet ou d'un programme de recherche clinique. Pour tout processus qui n'entre pas dans le champ d'application du présent Code de Conduite, la CRO et le Promoteur conservent le pouvoir discrétionnaire de conclure des arrangements contractuels particuliers, adaptés aux fins de ce processus particulier.

1.9 Le rôle de Sous-traitant

1.9.1 Justification dans le present code

Les rôles de responsable du traitement des données et de sous-traitant sont pris en compte dans le présent Code de Conduite dans le seul but de définir la relation qui doit être mise en place entre les promoteurs et une ou plusieurs CROs impliquées dans la même activité de recherche clinique en ce qui concerne leurs obligations respectives en relation avec le RGPD.

Selon le RGPD, le responsable du traitement est l'organisation qui définit les finalités et les moyens du traitement des données. Dans le cadre de la Recherche clinique, la Finalité est définie dans le protocole et les moyens sont définis (a) dans le protocole, (b) le plan de monitoring, (c) le plan de data management et (d) le plan d'analyse statistique.

Si l'on considère la relation contractuelle entre le promoteur et ses CROs sous-traitants, tous ces documents relèvent, conformément aux lignes directrices de l'ICH E6 (R2) sur les bonnes pratiques cliniques (BPC), de la responsabilité du promoteur.

Par conséquent, ce Code de Conduite aborde les schémas contractuels les plus courants dans lesquels le promoteur joue le rôle de responsable du traitement des données pour la recherche clinique et la CRO sous-traitante qui adhère à ce Code agit en tant que sous-traitant des données.

Quel que soit le rôle du professionnel de santé (PdS) et du Site Investigateur vis-à-vis du Promoteur, le présent Code s'applique de la même manière étant donné que le rôle du PdS ou du Site Investigateur au regard du RGPD n'a pas d'impact sur la conformité de la CRO au présent Code. Si le Promoteur charge la CRO de passer un contrat en son nom avec les professionnels de santé ou le Site Investigateur, alors la CRO sera toujours considérée comme le sous-traitant du Promoteur et le Code s'appliquera.

1.9.2 Exclusions de ce Code de Conduite

Le présent Code de Conduite ne vise pas à couvrir de manière exhaustive tous les schémas contractuels susceptibles de se produire entre un Promoteur et une CRO, et il n'existe pas une telle obligation pour un Code de Conduite de couvrir toutes les activités de l'industrie dans le RGPD.

Les parties prenantes de la recherche clinique, en particulier les promoteurs et les CROs, ont toujours la possibilité de s'engager mutuellement dans des relations où les responsabilités du responsable du traitement et du sous-traitant peuvent être réparties autrement que défini dans le présent code.

Exemples:

- Lorsque le promoteur et la CRO sont contractuellement engagés dans une responsabilité conjointe;
- Le promoteur et les sites investigateurs sont exclus;
- Une CRO qui fournit un service qui n'est pas couvert par les Classes de Services de ce code;

Le présent Code de Conduite ne s'applique pas à ces cas.

Cela ne signifie pas que de telles situations ne peuvent pas se produire. Si de telles situations se produisent, les organisations concernées mettent en place les dispositions contractuelles appropriées et ces dispositions ne sont pas régies par le présent Code de Conduite.

De manière générale, l'adhésion au Code n'empêche pas une organisation de se conformer au RGPD pour les activités qui peuvent être menées par ces organisations et qui ne sont pas régies par le présent Code de Conduite ou incluses dans son champ d'application.

1.9.3 Les principes de non-exclusivité et de non-équivalence

Le fait que le présent code n'envisage que les schémas contractuels dans lesquels le promoteur est le responsable du traitement et la CRO un sous-traitant, n'empêche pas les CROs sous-traitantes d'exercer des activités pour lesquelles elles ont le rôle de responsable du traitement, et n'exclut pas la possibilité qu'une même organisation exerce différentes activités pour lesquelles elle peut avoir différents rôles.

Exemples :

- Certaines activités où les Personnes concernées sont des membres du personnel de la CRO et où l'activité est liée à la gestion générale de ce personnel, sont des activités où la CRO agit en tant que responsable du traitement.
- Une CRO qui constitue et gère des bases de données contenant des informations sur des professionnels de la santé susceptibles d'être invités à participer à une future recherche clinique ne faisant pas encore l'objet d'un contrat avec un promoteur, agit en tant que responsable du traitement en ce qui concerne cette activité de traitement spécifique.

Sans préjudice d'une évaluation *ad hoc* par toute autorité de contrôle, le fait qu'une CRO exécute des processus pour lesquels elle agit en tant que responsable du traitement en dehors du contrat de service ne peut être interprété pour requalifier la position de cette CRO en responsable conjoint du traitement dans le cadre du contrat de service.

1.10 Principes et méthodologie de la Conformité

1.10.1 Une répartition claire des responsabilités en matière de Protection des données à caractère personnel

Conformément à l'article 82 "Droit à réparation et responsabilité" considérant 2 du RGPD.

> *[…] Le sous-traitant n'est responsable du dommage causé par le traitement que s'il […] a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.*

Ce code repose sur l'exigence que le Promoteur et la CRO doivent convenir d'une répartition claire des responsabilités en matière de protection des données, et tel est l'objet du contrat de service.

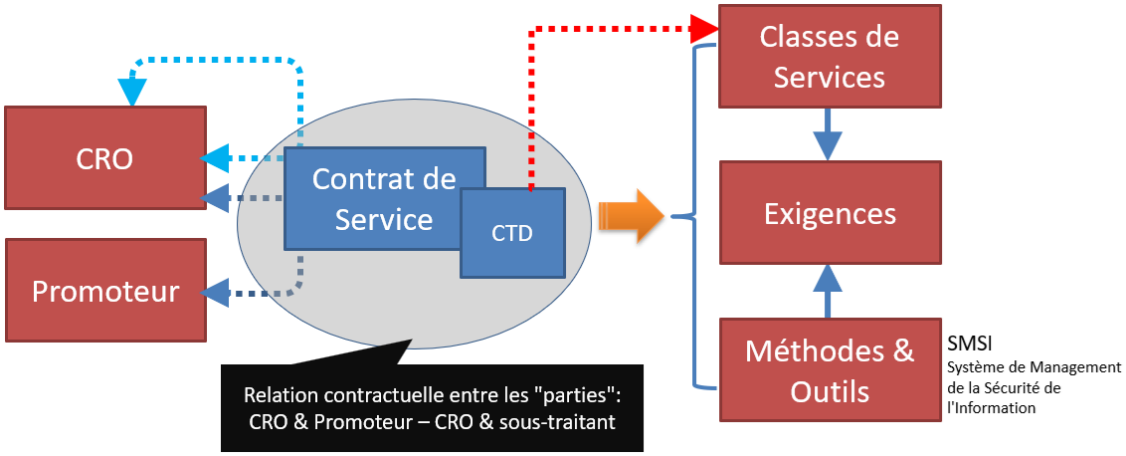
Le même régime s'applique lorsqu'une CRO sous-traite avec une autre CRO ou un autre prestataire pour certains des services qu'elle fournit au promoteur / responsable de traitement.

Les conditions relatives à la Protection des données à caractère personnel énoncées dans le Contrat de Service, constituent ensemble le contrat relatif au traitement des données (CTD) entre les parties au Contrat de Service. Ces conditions peuvent être incluses dans le contrat de service principal, par exemple sous forme d'annexe, ou dans un contrat séparé, comme illustré dans le diagramme ci-dessous.

Les conditions fixées dans le contrat de service ne doivent pas contredire la réglementation applicable et notamment le RGPD.

Au total, le Contrat de Service et le CTD joint, constituent la relation contractuelle établie entre la CRO et le Promoteur qui permettra d'identifier les responsabilités et les obligations respectives des parties en matière de protection des données en cas de litige ou d'action en justice.

Le présent Code repose sur le fait que ces responsabilités et obligations dépendent directement des services fournis par la CRO au promoteur. Le contrat de services doit obligatoirement définir les services et les produits livrables afférents fournis au promoteur par la CRO (ou le sous-traitant de la CRO).



Une répartition claire des responsabilités régie par une relation contractuelle.

Le "contrat de service" et le contrat relatif au traitement des données (CTD) adressent spécifiquement les questions de protection des données à caractère personnel.

1.10.2 Un schéma de conformité adapté au profil de chaque entreprise : Déclaration d'applicabilité

Ce code établit une liste d'exigences vis-à-vis desquelles la conformité est évaluée et contrôlée.

Au total, 216 exigences ont été spécifiées et répertoriées : 91 sont spécifiques au présent code et sont spécifiées dans le présent document ; 113 correspondent à des exigences de la norme ISO 27001 et 12 correspondent aux exigences de la norme ISO 27701.

Les CROs peuvent présenter des profils d'entreprises très différents, depuis de petites entreprises comptant quelques employés et fournissant des services très spécifiques (par exemple, des services de data management ou d'analyse biostatistique uniquement) jusqu'à de grandes multinationales avec une offre "tous services". La grande variété et l'hétérogénéité des services fournis est une spécificité du domaine de la recherche clinique. C'est pourquoi le Code a été conçu pour que le modèle de conformité d'une CRO adhérant au Code puisse être très différent de celui d'une autre CRO adhérant au Code.

Ainsi, une petite CRO fournissant un seul service avec un impact limité en termes de protection des données[4] et sans plateforme informatique en ligne dédiée n'a pas besoin de se conformer à l'ensemble des 216 exigences.

La conformité à ce Code dépend donc du profil de la CRO, défini par les catégories de services qu'elle vend à ses clients, qu'il s'agisse de promoteurs ou d'autres CROs. Si une CRO fournit une large gamme de services, elle peut demander l'adhésion pour tous les services, un seul ou plusieurs services sélectionnés.

L'annexe 2 ci-après énumère toutes les classes de services entrant dans le champ d'application du présent code. Le terme "classe" fait référence au fait que ces services sont décrits de manière "générique" et ne sont pas spécifiques aux méthodes / produits livrables particuliers développés par une CRO donnée.

C'est pourquoi la première exigence du code est formulée comme suit :

1.10.	Une CRO adhérente doit définir une déclaration d'applicabilité répertoriant toutes les catégories de services pour lesquelles la CRO adhérente déclare se conformer au Code.

La déclaration d'applicabilité de chaque CRO adhérente sera publique et publiée sur le site internet de l'EUCROF.

[4] Par exemple, la *conception du synopsis, du protocole et du cahier d'observations* ou la *sélection du site et le contrat.*

Le document 02 du code comprend une matrice qui met en correspondance toutes les catégories de services avec toutes les exigences correspondantes, comme illustré ci-dessous.

Déclaration d'Applicabilité / Exigences	Classe de Service 1	Classe de Service 2	Classe de Service 3	…	Classe de Service 20
Exigence 1	Oui		Oui		
	…		…		
Exigence "n"	Non		Oui		
…	…		…		

Exemple d'une CRO fournissant des services dans les classes 1 (Synopsis, conception du protocole et du cahier d'observations) et 3 (Sélection des sites investigateurs et contrats).

Cette approche permet à une CRO qui souhaite adhérer au Code, de ne prendre en compte que les exigences qui lui sont applicables. Elle facilite l'adhésion des CROs qui répondent à la définition des petites et moyennes entreprises telle que définie par la Commission Européenne[5] .

Le présent Code considère que les CROs souhaitant obtenir l'adhésion pour toutes les catégories de services énumérées doivent se conformer à toutes les exigences applicables du Code. La certification ISO 27001 est alors fortement recommandée bien que pas obligatoire.

Les exigences correspondant à la déclaration d'applicabilité d'une CRO adhérente ont une force contraignante et engagent donc contractuellement la responsabilité de ladite CRO à se conformer à ces exigences pendant la période d'adhésion au code.

Une CRO adhère au code lorsqu'elle démontre qu'elle se conforme à toutes les exigences énumérées correspondant au profil de son entreprise (c'est-à-dire à la déclaration d'applicabilité). Cela implique de documenter la manière dont la CRO se conforme à chacune des exigences applicables. Le cas échéant, il peut s'avérer nécessaire de joindre des documents supplémentaires tels que des procédures opératoires standardisées (SOP), des politiques ou des dossiers spécifiques, ainsi que la documentation relative à un système de management de la sécurité de l'information (SMSI).

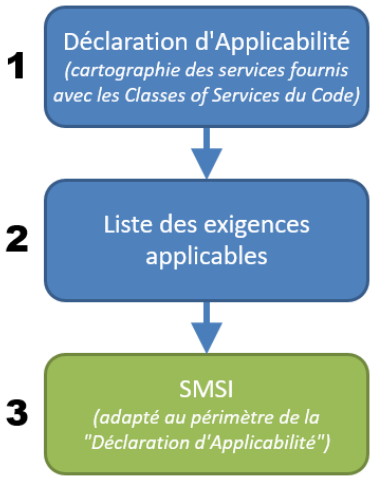
1.10.3 Toutes les CROs adhérentes doivent disposer d'un système de management de la sécurité de l'information (SMSI).

Le présent code tient compte du fait que la grande majorité des CROs, quelle que soit leur taille, disposent déjà d'un système de gestion de la qualité (SMQ) certifié ISO 9001:2015. Elles sont habituées à la collecte des enregistrements nécessaires pour démontrer le maintien, au cours du temps, d'un tel SMQ et en assurer l'amélioration continue.

Comme pour tout processus de conformité, les méthodes de conformité propres à la CRO doivent être dûment documentées et contrôlées au moyen d'enregistrements.

En vertu de ce code, la Conformité aux obligations de sécurité des sous-traitants doit être réalisée au moyen d'un SMSI - Système de Management de la Sécurité de l'Information tel que ceux illustrés dans les normes ISO 27001 et ISO 27701 (voir section 4.2 du code pour plus de détails).

[5] Voir https://ec.europa.eu/growth/smes/sme-definition_en.



La figure de gauche illustre les trois principales étapes de l'application du SMSI :

1 Établir la "déclaration d'applicabilité" de la CRO en mettant en correspondance les services fournis avec les classes de services figurant à l'annexe 2 du code ;

2 Analyser le document 02 du Code pour obtenir la liste des exigences du Code applicables à la CRO. Si une exigence doit être exclue, cette exclusion doit être identifiée et justifiée conformément à l'exigence 4.2.e ;

3 Documenter les mesures de conformité au moyen d'un Système Management de la Sécurité de l'Information (SMSI) correspondant à la Déclaration d'Applicabilité et maintenir ce système dans le temps (voir la section 4.2 du Code pour plus de détails).

1.10.4 Signification des marques de conformité au code EUCROF attribuées à une CRO

L'adhésion de la CRO lui confère le droit d'afficher une marque de conformité au Code EUCROF. Les marques de conformité au Code EUCROF sont disponibles pour deux niveaux d'adhésion différents. Comme décrit à la section 5 du Code, les CROs ont la possibilité de choisir le niveau d'adhésion souhaité.

Une marque de conformité au Code EUCROF de niveau 1 est attribuée aux CROs dont le dossier a été approuvé par le COSUP dans le cadre d'une procédure d'adhésion déclarative, et une marque de conformité au Code EUCROF de niveau 2 est attribuée aux CROs qui ont, en complément, fait l'objet d'un audit.

Pour obtenir l'une ou l'autre des marques de conformité au Code EUCROF, une CRO doit démontrer qu'elle respecte les exigences du Code correspondant à sa déclaration d'applicabilité.

Lorsqu'ils évaluent la marque de conformité au Code EUCROF d'une CRO, les promoteurs et autres parties prenantes, doivent prendre en considération la complexité de l'évaluation associée, ainsi que les ressources qui doivent être investies par la CRO au titre du processus d'évaluation correspondant.

2 Cadre général pour la protection des données à caractère personnel

2.1 Personnes concernées

Le présent Code définit les règles applicables au traitement des données à caractère personnel des groupes de personnes suivants :

1) Sujets d'étude
2) Professionnels de santé
3) Autres parties prenantes de l'étude

Les sujets d'étude comprennent la partenaire enceinte, le nouveau-né ou l'enfant à naître du sujet d'étude, ainsi que les membres de la famille, par exemple lorsqu'une étude envisage des recherches sur la génétique et l'hérédité.

Les professionnels de santé comprennent les investigateurs, les coordinateurs de l'étude, les infirmières et les autres membres du personnel qui participent directement à la recherche clinique.

D'autres parties prenantes de l'étude peuvent contribuer à la recherche et, par conséquent, leurs Données à caractère personnel peuvent également être recueillies dans les documents liés à l'étude. Ces personnes peuvent être des membres du personnel du promoteur de l'étude, des membres du personnel de la CRO, des représentants des autorités sanitaires, des représentants des patients, des conseillers médicaux, des membres des comités de gestion de la sécurité des données et des représentants des comités d'éthique.

2.2 Sources des données traitées

2.2.1 Sujets d'étude

En fonction de l'objectif de la recherche clinique et des instructions du promoteur, y compris comme spécifié dans le contrat de service, les CROs peuvent recevoir des données du sujet de l'étude de la part :

- Des professionnels de santé ;
- les sujets de l'étude eux-mêmes, par exemple par le biais des résultats rapportés par les patients ;
- Les représentants légaux du sujet de l'étude ;
- Les parents/membres de la famille du sujet de l'étude, par exemple au moyen d'un questionnaire ;
- Bases de données et/ou collections d'échantillons biologiques, légalement constituées et, le cas échéant, ayant fait l'objet des formalités nécessaires auprès des autorités compétentes ou pour lesquelles l'utilisation/l'accès est légalement autorisé. Ces ressources peuvent être accumulées à la suite d'études cliniques dans le cadre desquelles les personnes concernées ont donné leur consentement à l'utilisation de leurs échantillons biologiques restants et d'autres données générées au cours de l'étude "principale" à des fins de recherche future.

Conformément à la définition du sujet d'étude dans le présent Code, la portée des données à caractère personnel peut également inclure les données d'autres personnes, telles que la partenaire enceinte, le nouveau-né ou le membre de la famille agissant en tant que soignant du sujet participant à la recherche clinique. Cela signifie que dans le cadre de la recherche clinique et conformément au contrat relatif au traitement des données, la CRO peut collecter les données de ces personnes. Les données de ces personnes peuvent être collectées directement ou indirectement auprès du sujet de l'étude participant à la Recherche clinique.

Sauf instructions contraires du Promoteur et exigences des services/processus fournis, les CROs ne traitent pas de données permettant d'identifier directement le sujet de l'étude. Les sujets de l'étude ne sont identifiés que par un code d'identification propre à l'étude, ce qui constitue une pseudonymisation[6] conformément à l'article 4, paragraphe 5, du RGPD.

Les CROs peuvent également traiter des données à caractère personnel directement identifiantes pour des services complémentaires, selon les instructions du Promoteur, et sous réserve de garanties appropriées

[6] Avis n° 5/2014 du groupe de travail «Article 29» sur les techniques d'anonymisation ou toute version ultérieure de celui-ci

conformément à la section 3.6.3 du présent Code. Ces types de données peuvent être collectés auprès du professionnel de santé ou de la Personne concernée par l'étude elle-même.

Exemple :

Une CRO qui fournit aux patients un service de remboursement des frais de voyage et d'hébergement lors de visites à l'hôpital devra collecter des données à caractère personnel directement identifiantes des sujets de l'étude, telles que le nom, les coordonnées, les informations relatives au voyage, etc. Dans ce cas, une CRO ne devrait pas fournir les services qui impliquent un traitement parallèle de données relatives à la santé ou devrait mettre en œuvre des mesures de sécurité techniques et organisationnelles supplémentaires conformément à la section 3.6.3 du présent code. Ces mesures de sécurité visent à garantir la confidentialité de la Personne concernée par l'étude et à créer des pare-feu appropriés entre le personnel qui doit traiter des données à caractère personnel directement identifiantes et le personnel qui ne doit traiter que les données à caractère personnel pseudonymisées. De plus amples informations sur les services directement accessibles aux patients sont également fournies à l'annexe 2 - Classes de services relevant du champ d'application du présent code.

2.2.2 Professionnels de santé

Les données à caractère personnel des professionnels de santé sont nécessaires au Promoteur pour évaluer si les qualifications professionnelles et l'expérience du professionnel de santé correspondent aux besoins de l'étude. Un Promoteur peut également collecter des données à caractère personnel qui sont nécessaires à la communication avec les PdS, à l'organisation des transports liés à l'Étude vers le Site Investigateur et aux réunions investigateurs, etc. Lorsque la CRO traite des données à caractère personnel de membres du personnel de santé qui participent à l'étude clinique, ces données incluent des données directement identifiantes limitées à ce qui est nécessaire pour les finalités définies de l'étude. Il est évident que l'étendue des données ne comprendra pas les données relatives à la santé, contrairement à ce qui se passe dans le cas du traitement des données applicables aux sujets de l'Étude. Les données relatives aux professionnels de santé participant à la recherche clinique proviennent des Personnes elles-mêmes ou d'autres parties directement impliquées ou/et ayant la connaissance et l'intérêt professionnel et commercial légitime de fournir ces informations aux fins de la recherche clinique. Lorsqu'un promoteur fait participer des professionnels de santé à sa recherche, il est tenu d'informer ces derniers du traitement prévu ou effectif des données.

Exemples :

- Le promoteur fait appel à une CRO pour recruter des professionnels de santé et lui fournit la base de données des professionnels de santé du promoteur, qu'il conserve en tant que ressource interne ; la CRO et le promoteur conviennent contractuellement que la CRO élaborera des avis de protection des données et les fournira aux professionnels de santé pour le compte du promoteur.
- Un professionnel de santé peut recommander un collègue qui possède l'expérience et les qualifications professionnelles requises et qui pourrait être invité à faire partie de l'équipe de l'investigateur ; le promoteur/CRO ne reçoit du professionnel de santé que les coordonnées du collègue recommandé, toutes les autres données nécessaires à la recherche clinique étant obtenues directement auprès du professionnel de santé recommandé.

Dans les deux exemples, le promoteur est responsable de la notification aux prestataires de soins de santé. Toutefois, dans le premier exemple, il convient d'aligner le contenu de l'avis relatif à la protection des données à caractère personnel sur l'article 14 du RGPD. Dans le deuxième exemple, le contenu de l'avis doit être aligné sur l'article 13 du RGPD. La section 3.1 du code fournit des indications supplémentaires.

2.2.3 Autres parties prenantes de l'étude

Lorsqu'une CRO traite des données à caractère personnel d'autres parties prenantes de l'Étude qui sont impliquées dans la Recherche, ces données pourront inclure des données directement identifiantes mais pas des données relatives à la santé. Normalement, les données seront reçues soit directement des personnes concernées, soit de l'organisation qui emploie ces personnes.

Les données à caractère personnel de ces personnes sont utilisées à des fins de gestion de projet ; par exemple, l'équipe projet rend compte au personnel du promoteur de l'avancement de l'étude; la CRO confie à son personnel la responsabilité de faciliter la conduite de l'étude, et à cet effet, d'exécuter des tâches administratives et réglementaires; les équipes projet font des soumissions aux comités d'éthique et toutes autres soumissions règlementaires; les sous-traitants de la CRO fournissent aux professionnels de santé et au personnel du promoteur une assistance technique pour le logiciel utilisé dans la recherche etc. …

2.3 Responsabilité

Le promoteur, en tant que responsable du traitement des données, est tenu de pouvoir démontrer sa conformité au RGPD (principe de Conformité) et cette responsabilité s'étend à ses CROs sous-traitantes agissant en tant que sous-traitants qui ont leur propre responsabilité en vertu du RGPD (par exemple, l'article 82(2)).

Pour ces CROs sous-traitantes et sur la base (a) de la déclaration d'applicabilité publiquement disponible de la CRO et (b) du contrat de service et du contrat relatif au traitement des données qui y est joint énumérant les services sous-traités, l'adhésion au présent Code sera considérée comme un élément permettant de démontrer que la CRO se conforme bien aux exigences applicables du RGPD.

Lorsque la CRO engage un autre sous-traitant pour effectuer des activités de traitement pour le compte du sponsor, la CRO reste responsable des activités du sous-traitant vis-à-vis du promoteur.

Notes :

- Ce qui est exigé pour que le promoteur fasse preuve de responsabilité conformément au RGPD n'entre pas dans le champ d'application du présent code.
- La CRO, en tant que sous-traitant des données, doit suivre les instructions écrites fournies par le promoteur. Lorsque la CRO s'écarte de ces instructions écrites, elle sort du cadre du traitement des données et pourrait être considérée comme responsable du traitement.
- La CRO doit également être en mesure de produire d'autres documents, tels que la documentation conservée dans le SMSI, afin de démontrer la conformité au RGPD lorsque le promoteur ou un autre agent mandaté et désigné par le promoteur en fait la demande, conformément aux conditions d'audit énoncées dans le contrat de service et l'accord sur le traitement des données qui y est joint. La documentation produite doit être limitée au champ d'application du traitement que la CRO effectue pour le promoteur. À titre d'exemple, la CRO ne devra pas démontrer le respect de ses obligations au titre du RGPD en matière d'emploi car la CRO est le responsable du traitement des données à caractère personnel de son personnel.

2.4 Clauses relatives au traitement des données dans les contrats de service

Toutes les activités réalisées par les CROs (agissant en tant que sous-traitant, comme indiqué dans le champ d'application du présent Code de Conduite) pour le compte d'un Promoteur (agissant en tant que responsable du traitement) dans le cadre de la Recherche clinique sont régies par un contrat entre les deux parties qui doit être conforme aux exigences de l'article 28 du RGPD (ci-après le " Contrat de service ").

Les clauses relatives à la protection des données à caractère personnel conformes à l'article 28 du RGPD sont désignées dans le présent Code comme le " contrat relatif au traitement des données ".

Le contrat sur le traitement des données peut être un document autonome ou faire partie du contrat principal entre le Promoteur et la CRO. Quoi qu'il en soit, l'accord de traitement des données doit être explicitement considéré comme faisant partie intégrante du contrat de service et doit détailler toutes les obligations des parties concernant le traitement approprié des données à caractère personnel conformément aux exigences du RGPD et du présent Code de Conduite.

Domaine d'application : Les exigences expliquées dans chaque section du présent chapitre s'appliquent de manière générale, c'est-à-dire à toutes les classes de services énumérées à l'annexe 2, à l'exception des classes (1) et (2).

2.4.a Un contrat relatif au traitement des données juridiquement contraignant est conclu par écrit entre la CRO et le promoteur.

2.4.b Le contrat relatif au traitement des données est explicitement considéré comme faisant partie intégrante du contrat de service et doit être signé avant que toute activité de traitement des données ne soit effectuée par la CRO pour le compte du promoteur dans le cadre de la recherche clinique.

2.4.c Le contrat relatif au traitement des données détaille toutes les garanties requises pour la protection des données à caractère personnel conformément à l'article 28 du RGPD.

Dans le cas où il existe un Contrat Cadre de Services valable pour tous les projets sur lesquels le CRO travaille pour le compte du même Promoteur, un Contrat relatif au traitement des données spécifique n'est pas nécessaire pour chaque nouveau bon de commande émis par le Promoteur dans le cadre de ce Contrat Cadre de Services. Toutefois, les détails concernant la nature du traitement, les catégories de personnes concernées, les catégories de données à caractère personnel traitées, les sous-traitants, les mesures techniques et organisationnelles et les détails des transferts internationaux doivent être adaptés pour chaque activité de traitement que la CRO est chargée d'exécuter. Il est possible que ces détails soient inclus dans un ordre de travail qui relève du Contrat Cadre, plutôt que dans un Contrat du traitement des données qui fait partie du Contrat Cadre. Ce bon de commande devrait raisonnablement répondre aux exigences de l'article 28, paragraphe 3, du RGPD.

Exemples :

- Une CRO fournit des services de monitoring et de data management à un Promoteur et cette activité a fait l'objet d'un contrat cadre global. Ce Contrat Cadre prévoit qu'un bon de commande spécifique sera passé par le Promoteur chaque fois que la CRO participe à une nouvelle étude clinique. Le contrat relatif au traitement des données doit faire partie intégrante du Contrat Cadre et les conditions spécifiques qui s'appliquent à toute activité contractuelle particulière doivent être incluses dans le bon de commande.
- Une CRO fournit à un Promoteur une plateforme informatique en mode "Software as a Service" (y compris les activités de formation, d'assistance aux utilisateurs et de maintenance des logiciels par exemple) et cette activité fait l'objet d'un Contrat de service global. Le contrat relatif au traitement des données peut être inclus dans le contrat de service global. Les dispositions de l'accord relatif au traitement des données couvrent toutes les recherches cliniques effectuées par le promoteur à l'aide de la plateforme informatique et il n'est pas nécessaire de conclure un accord spécifique relatif au traitement des données pour chaque étude clinique effectuée par le promoteur à l'aide de cette plateforme informatique.

Les modèles de contrats relatifs au traitement des données proposés par l'EUCROF peuvent être insérés dans les contrats de service lorsque les parties sont respectivement le responsable du traitement / le sous-traitant / le sous-traitant du sous-traitant. Ces documents sont fournis à titre d'exemples non obligatoires et peuvent être utilisés comme base écrite contraignante pour la répartition des responsabilités en matière de protection des données à caractère personnel, convenue entre les parties au contrat de service. Une CRO peut également utiliser ses propres modèles de contrats relatifs au traitement des données, sous réserve de respecter les dispositions du présent Code.

Des informations supplémentaires sur les conditions d'utilisation de ces modèles de contrats relatifs au traitement des données sont disponibles dans une note additionnelle qui peut être téléchargée depuis le site internet de l'EUCROF par les CROs qui déposent une demande d'adhésion. Les modèles de contrats relatifs au traitement des données proposés par l'EUCROF sont considérés comme des documents autonomes, indépendants du présent Code.

Les principales exigences relatives à tout contrat au traitement des données sont énumérées ci-après :

2.4.d Le contrat relatif au traitement des données délimite les rôles et les responsabilités des deux parties.

2.4.e Le contrat relatif au traitement des données est valable pour toute la durée de la prestation de services de traitement des données à caractère personnel par la CRO et ne peut être résilié, sauf si d'autres accords régissant la prestation de services de traitement des données à caractère personnel ont été conclus entre la CRO et le promoteur ou si les services sont résiliés. Le contrat relatif au traitement des données doit comporter une exigence de survie des obligations de confidentialité après la résiliation, pour autant qu'elles ne s'appliquent pas aux demandes légitimes de divulgation émanant des autorités de contrôle de la protection des données.

2.4.f Le contrat relatif au traitement des données identifie clairement les activités de traitement couvertes.

2.4.g Le contrat relatif au traitement des données définit clairement les responsabilités du sous-traitant en matière de réponse aux demandes des personnes concernées, en tenant compte de l'exigence prévue à la section 3.6.1.a du présent code, et détaille les mesures techniques et organisationnelles que la CRO doit mettre en place pour aider le promoteur à s'acquitter de son obligation de répondre aux demandes d'exercice des droits des personnes concernées.

2.4.h Le contrat relatif au traitement des données précise que le sous-traitant ne peut pas utiliser les données de l'étude clinique à ses propres fins.

2.4.i Si le sous-traitant considère qu'une instruction du responsable du traitement enfreint les lois et règlements applicables, le contrat relatif au 'traitement des données précise que le sous-traitant doit en informer le responsable du traitement et cesser de suivre/appliquer cette instruction.

2.4.j Le contrat relatif au traitement des données identifie clairement le service que le sous-traitant des données fournira au responsable du traitement des données en vertu de l'article 28, paragraphe 3, points e) à f) du RGPD ; y compris :

- Le sous-traitant aide le responsable du traitement à réaliser l'analyse d'impact relative à la protection des données (AIPD).
- Le sous-traitant s'engage à aider le responsable du traitement au cas où une consultation des autorités de contrôle concernées serait exigée avant l'achèvement de l'AIPD.

2.4.k Le contrat relatif au traitement des données doit, conformément aux dispositions de l'article 28(3)(a) du RGPD, interdire au sous-traitant des données de transférer des données à caractère personnel vers un pays tiers sans instructions écrites préalables du responsable du traitement, à moins que le sous-traitant des données ne soit tenu de le faire en vertu du droit de l'Union ou de l'État membre auquel le sous-traitant des données est soumis. Le sous-traitant est tenu d'informer le responsable du traitement, avant le traitement, des exigences juridiques applicables en vertu du droit de l'Union ou de l'État membre auquel il est soumis entraînant le transfert de données à caractère personnel vers un pays tiers ou une organisation internationale, à moins que ce droit n'interdise une telle information pour des motifs importants d'intérêt public.

L'accord sur le traitement des données contient des instructions relatives au transfert des données à caractère personnel vers un pays tiers[7] faisant référence aux mécanismes de transfert spécifiques envisagés par le chapitre V du RGPD et dont le responsable du traitement des données approuve l'utilisation.

[7] Lignes directrices 05/2021 du CEPD sur l'interaction entre l'application de l'article 3 et les dispositions relatives aux transferts internationaux conformément au chapitre V du RGPD.

2.4.l Le contrat relatif au traitement des données définit les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel en tenant compte des risques spécifiques du traitement pour les droits des personnes concernées, en particulier des sujets de l'étude dont les données à caractère personnel traitées dans le cadre de la recherche clinique comprennent des catégories particulières de données à caractère personnel.

2.4.m Le contrat relatif au traitement des données prévoit l'obligation pour le Sous-traitant des données de notifier au responsable du traitement des données à caractère personnel toute violation de données à caractère personnel dès qu'il en a eu connaissance.

2.4.n Le contrat relatif au traitement des données doit préciser que toutes les données à caractère personnel doivent être renvoyées au responsable du traitement des données et que toutes les copies existantes doivent être détruites par le sous-traitant à la fin du Contrat de service, ou détruites sur demande et à la discrétion du responsable du traitement des données, à moins que la CRO ne soit soumise à des obligations pertinentes en vertu du droit de l'Union ou de l'État membre exigeant que la CRO stocke les données à caractère personnel.

2.4.o Le contrat relatif au traitement des données impose au Sous-traitant de former son personnel au traitement des données à caractère personnel au moins une fois par an et de fournir un certificat de formation qui sera inclus dans le dossier de documentation disponible en cas d'audit.

2.4.p Le contrat relatif au traitement des données oblige le sous-traitant à mettre à la disposition du responsable du traitement la liste de son personnel autorisé à accéder aux catégories particulières de données traitées dans le cadre du contrat relatif au traitement des données.

2.4.q Le contrat relatif au traitement des données oblige le sous-traitant à obtenir l'engagement individuel de confidentialité du personnel concerné qui traite les données à caractère personnel faisant l'objet de l'accord sur le traitement des données.

Remarque :

- Dans le cadre du présent code, lorsque la CRO est une des parties des contrats avec les Sites Investigateurs agissant en tant que Sous-traitants, le Promoteur reste le responsable du traitement des données. Dans ces contrats, la responsabilité du responsable du traitement ne peut être transférée à la CRO qui reste dans son rôle de sous-traitant des données. La présente note est sans préjudice du rôle du Site Investigateur dans le cadre du RGPD.

Exemple

- L'incorporation d'une clause d'obligation de confidentialité dans le contrat de travail (ou le contrat du freelance) peut être l'une des mesures mises en œuvre.

2.5 Clauses applicables aux sous-traitants ultérieurs

Dans le cadre d'une Recherche clinique, la CRO peut être amenée à solliciter ses propres sous-traitants pour répondre aux besoins de la Recherche clinique et doit s'assurer que ces sous-traitants s'engagent à fournir des garanties suffisantes conformément à l'article 28(4) du RGPD, comme expliqué à la section 4.4 du présent Code, dans la mesure où ces prestataires de services traitent des données à caractère personnel pour les besoins de l'Étude clinique. Des exemples de ces sous-traitants ultérieurs sont les laboratoires centralisés, les fournisseurs de solutions eCRF/ePRO, le prestataire de services de pharmacovigilance, le moniteur indépendant et le biostatisticien, la société assurant le transport/la logistique ou l'archivage, etc. Dans tous ces cas, le promoteur, en tant que responsable du traitement, doit être informé en temps utile de l'intention de la CRO de passer un contrat avec un sous-traitant ultérieur.

Exemple

- Le CRO tient à jour une liste des sous-traitants sur son site web, y compris la date de la dernière modification de la liste, et envoie une notification à tous les Promoteurs 30 jours avant l'ajout d'un nouveau sous-traitant, afin de donner au Promoteurs la possibilité de s'opposer à l'ajout d'un nouveau sous-traitant. Dans cet exemple, le contrat relatif au traitement des données doit encore être modifié pour intégrer le nouveau sous-traitant ultérieur, conformément à l'exigence 2.5.b du présent code.

Domaine d'application : Les exigences expliquées dans chaque section du présent chapitre s'appliquent de manière générale, c'est-à-dire à toutes les catégories de services énumérées à l'annexe 2, à l'exception des classes (1) et (2).

Les éléments suivants sont également couverts par le contrat relatif au traitement des données conclu entre le promoteur et la CRO :

2.5.a Le contrat relatif au de traitement des données doit inclure l'engagement à ne pas sous-traiter d'activités de traitement des données sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement des données et l'exécution d'un contrat avec ses sous-traitants autorisés qui comprend toutes les conditions applicables du présent Code de Conduite et, en particulier, les engagements à fournir des garanties suffisantes conformément à l'article 28, paragraphe 4, du RGPD[8] . Lorsqu'une autorisation spécifique est exigée, le contrat relatif au traitement des données doit inclure le processus d'obtention de cette autorisation.

Remarque :

- Contrairement à une autorisation spécifique, où le sous-traitant doit obtenir l'approbation du responsable du traitement pour chaque sous-traitant ultérieur, dans le cas d'une autorisation générale, le sous-traitant doit informer le responsable du traitement en temps utile de tout ajout ou remplacement envisagé de sous-traitant ultérieur, afin de donner au responsable du traitement la possibilité de s'y opposer. Le silence du responsable du traitement et/ou l'absence d'objection dans le délai imparti peuvent être interprétés comme une autorisation.

2.5.b Le contrat relatif au traitement des données conclu entre le responsable du traitement et la CRO identifie tous les sous-traitants désignés par la CRO comme étant nécessaires à la prestation de ses services et est réputé accepté par le responsable du traitement dès la signature du contrat de traitement des données. Si des sous-traitants supplémentaires sont envisagés après la signature du contrat relatif au traitement des données, le responsable du traitement doit être informé ou les accepter dans un avenant à l'accord entre les parties[9] qui est concerné, selon les dispositions prévues au contrat, qu'elles soient générales ou requièrent une autorisation écrite particulière.

Remarque :

- La liste des Sous-traitants est incluse dans le contrat relatif au traitement des données lui-même ou dans une annexe à l'accord et tenue à jour, conformément à l'autorisation générale ou spécifique donnée par le responsable du traitement. Cette liste des sous-traitants ultérieurs prévus comprend au moins, pour chaque sous-traitant ultérieur, le lieu où il se trouve et le type de services qu'il fournit. Les garanties mises en œuvre par les sous-traitants ultérieurs assurent le même

[8] Lignes directrices de la CEPD 07/2020 sur les concepts de responsable du traitement et de sous-traitant au titre du RGPD.
[9] Lignes directrices de la CEPD 07/2020 sur les concepts de responsable du traitement et de sous-traitant au titre du RGPD.

niveau de protection que celui assuré par le sous-traitant. Une liste des garanties incluses dans le contrat relatif au traitement des données entre le sous-traitant et le responsable du traitement est considérée comme une preuve des garanties mises en œuvre par les sous-traitants ultérieurs.

2.5.c Le contrat relatif au relatif au traitement des données conclu entre le responsable du traitement et la CRO définit la procédure à suivre pour ajouter, supprimer ou modifier l'un des sous-traitants secondaires énumérés, en accordant au responsable du traitement un délai raisonnable pour examiner les modifications proposées par la CRO et s'opposer aux nouveaux sous-traitants ultérieurs.

Les éléments suivants sont couverts par le contrat relatif au traitement des données conclu entre CRO et son sous-traitant :

2.5.d Les mêmes obligations en matière de protection des données que celles énoncées dans le contrat relatif au traitement des données entre le responsable du traitement et la CRO, comme spécifié à la section 2.4, sont incluses dans le contrat entre la CRO et ses propres sous-traitants ultérieurs, en particulier en fournissant des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées comme l'exige le RGPD et les procédures de désignation d'autres sous-traitants ultérieurs.

2.5.e Le contrat relatif au traitement des données conclu entre la CRO et ses propres sous-traitants identifie clairement les activités de traitement couvertes.

2.5.f Le contrat relatif au traitement des données entre la CRO et ses propres sous-traitants ne doit pas permettre au sous-traitant de transférer des données à caractère personnel vers un pays tiers, à moins que le sous-traitant n'ait mis en œuvre un mécanisme juridique pour le transfert de données conformément aux articles 44-49 du RGPD. En cas de transfert (ultérieur ou autre) par son sous-traitant, la CRO doit s'assurer que son sous-traitant ultérieur a mis en œuvre un mécanisme juridique pour le transfert de données et a démontré la mise en œuvre de ces garanties avant de transférer des données à caractère personnel à un Pays tiers, conformément à la section 4.6 du Code.

Remarque :

- Lorsqu'un sous-traitant de la CRO ne remplit pas ses obligations en matière de protection des données, la CRO reste pleinement responsable vis-à-vis du responsable du traitement de l'exécution des obligations de ce sous-traitant. Néanmoins, cette responsabilité n'empêche pas le sous-traitant défaillant d'être directement sanctionné par les autorités de protection des données. La CRO pourra également intenter une action contre le sous-traitant défaillant.

Les dispositions suivantes s'appliquent généralement à la sous-traitance :

2.5.g La CRO fournit une copie des contrats relatifs au traitement des données conclus entre elle-même et les sous-traitants ultérieurs à la demande du responsable du traitement ou de l'Autorité de contrôle compétente, afin de démontrer qu'il existe des garanties suffisantes.

2.6 Obligations de confidentialité

L'article 28 du RGPD prévoit que [...] *le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel se soient engagées à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;*

Domaine d'application : Les exigences expliquées dans chaque section du présent chapitre s'appliquent de manière générale, c'est-à-dire à toutes les catégories de services énumérées à l'annexe 2.

2.6.a Les CROs veillent à ce que leurs employés soient soumis à une obligation de confidentialité, soit dans leur contrat de travail, soit dans un accord de confidentialité distinct, soit dans tout autre mécanisme d'engagement équivalent, et qu'ils soient suffisamment informés et formés pour exercer ce devoir conformément au RGPD et aux normes et politiques correspondantes de l'entreprise.

Notes :

- Cette exigence s'applique également aux free-lances et, d'une manière générale, à tous les sous-traitants avec lesquels les CROs coopèrent pour fournir les services assignés.
- Voir également les exigences 2.4.o, 2.4.p et 2.4.q ci-dessus.

2.6.b Les CROs et les sous-traitants secondaires mettent en œuvre, documentent et contrôlent toutes les mesures techniques et organisationnelles visant à garantir que les obligations de confidentialité sont respectées de manière appropriée par leurs employés.

Exemple :

- Un manuel de l'employé ou un document similaire contient des dispositions sur les actions disciplinaires et les sanctions qui peuvent être prises conformément au droit du travail applicable si les employés ne respectent pas le devoir de confidentialité. Les sanctions ou actions disciplinaires peuvent inclure des avertissements verbaux ou écrits, une nouvelle formation, un rapport documenté de la part de leur responsable fonctionnel, la résiliation du contrat de travail (conformément à la réglementation applicable), ou toute autre action légale appropriée entreprise par l'organisation employeuse, etc.

2.7 Instructions du responsable du traitement

L'article 28 du RGPD précise que [...] *le sous-traitant traite les données à caractère personnel uniquement sur instructions documentées du responsable du traitement ;*

Domaine d'application : Les exigences expliquées dans chaque section du présent chapitre s'appliquent de manière générale, c'est-à-dire à toutes les classes de services énumérées à l'annexe 2.

Dans le présent code, le terme "documenté" s'entend uniquement comme "écrit" (électroniquement ou non) et avec une identification claire du responsable du traitement auteur de l'instruction, ainsi qu'une identification claire du contrat de service en vertu duquel ladite instruction est diffusée.

Si le contrat de service et l'accord de traitement des données correspondant sont conçus pour établir clairement les responsabilités respectives des parties (responsable du traitement et sous-traitant) d'une manière conforme au RGPD, des registres sont conservés pour démontrer que chaque partie a continuellement agi en conséquence et que toutes les instructions essentielles du promoteur / responsable du traitement ont pris une forme écrite formelle, comme l'exige l'article 28 du RGPD.

En cas de litige ou d'action en justice, d'inspection ou d'audit de sécurité interne, ces registres sont rapidement mis à disposition par la CRO.

Comme rappelé à la section 2.3 ci-dessus (et à condition que ces instructions soient conformes au RGPD et fixées dans le contrat de service), "*lorsque la CRO s'écarte de ces instructions écrites, elle agit au-delà du champ d'application d'un sous-traitant de données et peut être considéré comme responsable du traitement*".

Ces documents peuvent être considérés comme faisant partie du Trial Master File (TMF), que ces instructions soient spécifiques à l'étude ou non. On entend par document toute instruction écrite fournie par le promoteur à la CRO, par exemple un mémorandum, un courrier électronique ou tout autre moyen écrit pouvant être attribué au responsable du traitement. Le terme "essentiel", qui est ajouté ici pour définir quelles instructions doivent prendre une forme écrite, doit être compris dans le même sens que pour le TMF, mais il peut appartenir aux parties de préciser dans le contrat de service ou le contrat relatif au traitement des données quelles instructions doivent prendre une forme écrite et quelle doit être cette forme.

2.7.a Les CROs veillent à ce que le traitement des données à caractère personnel effectué dans le cadre du contrat de service ne soit réalisé que conformément aux instructions écrites du promoteur agissant en qualité de responsable du traitement et à ce que ces instructions écrites soient enregistrées dans son système de documentation et puissent être facilement produites en cas d'audit.

Remarque :

- La CRO peut inclure dans ses politiques et procédures standard une liste de tous les types d'instructions qui doivent être obtenues par écrit de la part des promoteurs, ainsi que les modèles associés.

2.7.b La CRO veille à ce que les instructions écrites émanant du responsable du traitement comportent au minimum une identification sans ambiguïté du responsable du traitement, du contrat de service en vertu duquel cette instruction est émise, ainsi que du processus et/ou du service concerné.

La raison de cette exigence est qu'en cas d'inspection, de litige ou de base juridique, le document écrit doit fournir des motifs clairs pour la prise de décision et le contrôle.

Le promoteur /responsable du traitement et la CRO / sous-traitant peuvent tous deux être confrontés à des situations où une instruction écrite du promoteur entre dans le champ d'application du contrat de service, mais où sa conformité au RGPD fait éventuellement l'objet d'interprétations différentes.

2.7.c L'accord relatif au traitement des données signé par le promoteur et la CRO doit prévoir une règle claire sur la manière de gérer les situations dans lesquelles une instruction écrite du responsable du traitement, conformément à la section 4.5 du Code, est considérée par la CRO comme non conforme au RGPD ou/et à d'autres dispositions réglementaires et légales de l'Union ou de l'État membre en matière de protection des données. Si un tel cas se produit, la CRO a la possibilité d'obtenir une décharge écrite pour éviter tout engagement de sa responsabilité ou de suspendre l'exécution des instructions en question jusqu'à ce que ces instructions aient été soit clarifiées, soit modifiées pour être conformes au RGPD ou aux réglementations applicables.

Notes :

- Dans tous les cas, ces instructions écrites s'inscrivent dans le cadre du contrat de service.
- Les informations écrites communiquées par la CRO au promoteur et l'avis de non-responsabilité qui en découle doivent être archivés dans le système de documentation de la CRO et être facilement accessibles en cas d'audit.

3 Application des principes de protection des données aux CROs

Ce chapitre transpose de manière pratique et dans le cas spécifique des activités des CROs, les exigences générales du RGPD. Il est néanmoins rappelé que, dans tous les cas, l'adhésion au Code n'exonère pas la CRO de devoir respecter tous les principes du RGPD, y compris pour ses activités qui ne sont pas régies par le présent Code de Conduite ou incluses dans son champ d'application.

Une CRO adhérente doit mener sa propre analyse juridique pour déterminer s'il existe des circonstances autres que celles envisagées dans ce Code dans lesquelles elle devrait appliquer les principes du RGPD.

3.1 Licéïté, loyauté et transparence

Cette section fait référence à l'article 5 du RGPD, qui stipule que "les *données à caractère personnel sont : a) traitées* ***licitement, loyalement et de manière transparente à l'égard de la*** *personne concernée* ("licéité, loyauté et transparence") et aux articles 12, 13 et 14 du RGPD qui définissent les informations à fournir à la personne concernée.

Pour satisfaire à ces obligations, le Sponsor agissant en tant que responsable du traitement est chargé de fournir des informations détaillées aux personnes concernées sur le traitement de leurs données à caractère personnel aux fins de l'Étude, d'expliquer la base juridique du traitement, d'obtenir le consentement à l'utilisation des données si le consentement est la base juridique du traitement des données, et de veiller à ce que l'exécution de ces obligations puisse être démontrée. Le Sponsor peut faire appel à une CRO pour fournir ces services et exiger de ce dernier qu'il l'aide à se conformer à ces responsabilités.

Domaine d'application. Les exigences de cette section s'appliquent aux CROs qui fournissent un ou plusieurs des services suivants listés dans l'annexe 2 :

- (2) Formulaire de consentement éclairé et notice d'information
- (3) Sélection du site et contrat
- (4) Collecte des données
- (8) Services aux patients
- (22) Activités réglementaires/de démarrage
- (23) Organisation des réunions investigateurs

Dans le cadre de sa responsabilité au titre du principe de transparence, une CRO doit élaborer une politique garantissant au responsable du traitement son aide pour fournir aux personnes concernées des informations complètes sur l'utilisation des données.

3.1.a Sur la base des informations fournies par le promoteur, la CRO aide le promoteur dans l'élaboration, la communication et la distribution d'informations sur le traitement des données aux personnes concernées et dans l'obtention du consentement au traitement des données à caractère personnel auprès des personnes concernées, lorsque ce traitement repose sur le consentement en tant que base légale. Tous les processus et documents élaborés par la CRO pour le compte du promoteur doivent être approuvés par ce dernier avant que la CRO ne puisse les utiliser ou les diffuser.

3.1.b Les CROs doivent disposer de processus et de procédures internes décrivant la distribution des avis de confidentialité du promoteur aux professionnels de santé dans le cadre des études de faisabilité, des visites d'initiation des sites, etc.

Exemple :

- Une CRO fournissant des services aux patients (voir la liste des services à l'annexe 2) peut disposer de modèles de notices d'information/de formulaires de consentement pour aider les responsables du traitement à s'acquitter de leurs responsabilités en matière d'information des personnes concernées sur le traitement de leurs données à caractère personnel.
- Une CRO qui reçoit les données à caractère personnel des professionnels de santé d'un tiers plutôt que de la personne elle-même fournira un avis de confidentialité à ce professionnel de santé avec, en particulier, la source des données et des détails sur la façon de s'opposer au traitement de leurs données.

Base juridique du traitement des données et informations à fournir aux personnes concernées

Lorsqu'une CRO participe à l'élaboration des formulaires de consentement éclairé (FCI) et des brochures d'information destinés aux sujets de l'étude et à la sélection des professionnels de santé, elle s'en remet à l'avis du responsable du traitement sur la base juridique appropriée pour le traitement des données, étant donné qu'il incombe au responsable du traitement de définir cette base. La CRO inclura cette information dans les sections pertinentes du consentement éclairé et des brochures d'information fournies aux sujets de l'étude, ainsi que dans les notifications aux professionnels de santé.

3.2 Limitation des finalités

Cette section fait référence à l'article 5 du RGPD, qui stipule que *"Les données à caractère personnel sont : b) collectées pour des **finalités déterminées, explicites et légitimes**, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ; le traitement ultérieur à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (**"limitation des finalités"**)";*

3.2.1 Utilisation primaire

Le principe de limitation des finalités fixe les limites des finalités pour lesquelles les données à caractère personnel peuvent être traitées, étant donné qu'en vertu de ce principe : i) les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ii) ne pas être traitées ultérieurement de manière incompatible avec ces finalités.

Afin de démontrer la bonne mise en œuvre de ce principe dans le cadre des services fournis au promoteur, la CRO doit élaborer une politique traitant du principe de limitation des finalités et garantissant sa mise en œuvre au moyen de pratiques, de procédures et de formulaires de saisie des données.

Domaine d'application : Les exigences détaillées dans cette section s'appliquent à toutes les classes de services listées à l'annexe 2, à l'exception des classes (1) et (2) et (17).

3.2.1.a Avant de commencer le traitement, la CRO vérifie que toutes les données à caractère personnel qu'elle doit traiter seront collectées conformément au protocole de chaque étude clinique.

Notes :

- Une CRO est censée examiner le protocole et comparer les critères d'évaluation énumérés avec les données collectées et évaluer s'il y a des données qui n'ont pas trait au protocole de recherche.
- Une CRO qui fournit des services de conception de synopsis, de protocoles et d'eCRF (voir la liste des services à l'annexe 2) est censé intégrer dans ses politiques et procédures des dispositions sur la manière dont il forme le personnel dont les responsabilités consistent à créer ces documents ; ces dispositions doivent expliquer les critères, les normes et les matrices permettant d'intégrer les règles relatives au contrôle des utilisations des données de l'étude clinique par le biais de la conception de ces documents d'étude.

Dans le domaine de la Recherche clinique, la Finalité première du traitement des données à caractère personnel est la réalisation des objectifs poursuivis par le protocole de chaque Étude clinique. Ainsi, l'utilisation primaire des données de l'étude clinique comprend toutes les opérations de traitement liées à un protocole d'étude clinique spécifique, pendant tout son cycle de vie, depuis le début de l'étude clinique jusqu'à la suppression, à la fin de la période d'archivage.

3.2.2 Utilisation secondaire

Les traitements relevant de cette section sont ceux qui visent à utiliser les données à caractère personnel collectées dans le cadre d'une étude clinique à des finalités secondaires, à savoir à des fins autres que celles définies par le protocole de l'étude clinique. Toute utilisation secondaire de données à caractère personnel à des fins de recherche scientifique doit être évaluée par le responsable du traitement.

Exemples :

- Un promoteur souhaite utiliser les données médicales collectées lors d'un essai clinique sur le cancer de la prostate pour mener une étude visant à identifier de nouveaux biomarqueurs, ce qui n'était pas prévu dans le protocole de l'étude clinique.
- Un promoteur décide d'utiliser des données d'étude pseudonymisées obtenues au cours d'études antérieures à des fins de recherche scientifique, par exemple pour le développement de nouveaux algorithmes d'intelligence artificielle, afin d'améliorer les approches diagnostiques ou les méthodologies d'évaluation des maladies.

Un sous-traitant n'est pas autorisé à utiliser les données à caractère personnel qu'il traite à des fins secondaires, sauf instruction/autorisation du responsable du traitement. Conformément à la section 2.3, une CRO qui agit au-delà des instructions du responsable du traitement peut être considérée comme assumant le rôle de responsable du traitement pour la nouvelle finalité, ce qui signifie qu'elle doit également accepter les obligations d'un responsable du traitement et prendre des mesures pour s'en acquitter.

3.2.2.a Dans les cas où la CRO est chargée par le Sponsor de traiter des données à caractère personnel en dehors du protocole original de l'Étude, la CRO doit :

1) Veiller à ce que le traitement soit effectué conformément à un contrat qui couvre les finalités secondaires du traitement en modifiant les accords précédents ou en concluant un nouveau contrat ; et
2) Adopter les mesures techniques et organisationnelles appropriées du présent Code afin que la CRO puisse traiter en toute sécurité les données à caractère personnel à des fins secondaires.

Exemples :

- Un promoteur décide de réanalyser des données qui ont déjà été collectées pour une finalité secondaire compatible avec les finalités initiales selon l'évaluation du responsable du traitement. La CRO veille à ce que le traitement soit effectué conformément à un contrat approprié et respecte les obligations qui en découlent, y compris, en particulier, en fournissant une assistance au promoteur pour l'élaboration et l'envoi de l'information aux personnes concernées conformément aux articles 13 et 14 du RGPD ainsi que pour l'application de mesures techniques et organisationnelles appropriées.

L'utilisation secondaire de données totalement anonymes ne relève pas du champ d'application du présent code. Il convient de noter que le procédé d'anonymisation doit également s'appuyer sur une base juridique valable conformément à l'art. 29 de l'avis 05/2014 du groupe de travail sur les techniques d'anonymisation (ou toute version ultérieure).

3.3 Minimisation des données

Cette section fait référence à l'article 5 du RGPD, qui stipule que *" les données à caractère personnel sont : c)* ***adéquates, pertinentes et limitées à ce qui est nécessaire au regard*** *des finalités pour lesquelles elles sont traitées (****" minimisation des données "****).*

Le responsable du traitement (promoteur) exigera que la CRO s'aligne sur les principes de minimisation des données et de respect de la vie privée dès la conception et par défaut. L'alignement sur ces principes clés contribuera à garantir la protection des droits et des libertés des personnes concernées. Seules les activités liées à la réalisation de l'étude clinique ou à d'autres services spécifiques pour le promoteur entrent dans le champ d'application de ces principes clés.

Pour démontrer sa responsabilité dans la mise en œuvre du principe dans ses pratiques, une CRO doit élaborer une politique expliquant comment le principe de minimisation des données est intégré dans les services qu'elle fournit aux commanditaires.

Domaine d'application : Les exigences de la présente section s'appliquent à toutes les classes de services de l'appendice 2, à l'exception de (17) Fourniture d'une infrastructure physique d'hébergement ou comme indiqué dans le document 02.

Exemple :

- Une CRO qui fournit des services de conception de synopsis, de protocole et de CRF (voir la liste des services à l'annexe 2) doit prévoir une formation spéciale sur la minimisation des données pour ses employés et fournir un rapport d'analyse sur la minimisation des données dans les documents livrés avec le protocole et le(s) CRF(s).

En vertu du principe de minimisation des données, la CRO ne collecte que des données à caractère personnel adéquates, pertinentes et limitées à ce qui est nécessaire aux fins du traitement. Plus précisément, la CRO ne traite que les données à caractère personnel qui sont nécessaires pour mener à bien les activités de traitement selon les instructions du promoteur.

3.3.a La CRO aide le promoteur en ne collectant que les données à caractère personnel qui sont nécessaires, conformément aux instructions écrites du promoteur et aux finalités au moment de la collecte. Les données à caractère personnel qui ne sont pas nécessaires à l'exécution des instructions écrites du promoteur ne sont pas collectées et traitées par la CRO en tant que responsable de la mise en œuvre du traitement des données.

3.3.b La CRO fournit, dans la mesure de ses compétences et de son expertise spécifiques, toute l'aide demandée par le promoteur pour définir les données à caractère personnel adéquates, pertinentes et nécessaires au regard des finalités pour lesquelles elles sont traitées.

Le promoteur peut exiger de la CRO qu'elle fournisse des outils pour mener à bien les activités de traitement, comme spécifié dans des instructions écrites. Ces outils peuvent être créés et entretenus par la CRO ou être le produit ou le service obtenu auprès d'une autre partie.

3.3.c En ce qui concerne le respect de la vie privée dès la conception et par défaut, la CRO veille à ce que les outils de traitement soient en mesure de prendre en charge les principes de minimisation des données, les exigences de limitation du stockage et de faciliter les droits des personnes concernées, conformément aux instructions du promoteur.

Notes :

- Une CRO qui fournit un système d'EDC concevra des formulaires de rapport de cas qui, techniquement, ne permettent pas la saisie de données à caractère personnel non requises par le protocole de l'étude, par exemple en réduisant au minimum les champs de texte libre, en incluant des champs fixes indiquant quels types de données doivent être saisis, ou en prévoyant des champs pour la saisie de l'année de naissance ou de l'âge plutôt que de la date de naissance complète. De cette manière, seules les données à caractère personnel nécessaires seront saisies et les informations inutiles susceptibles de contenir des catégories particulières de données à caractère personnel ne seront pas traitées.
- Dans le cadre du point (23) "Organisation des réunions investigateurs", la CRO doit veiller à ce que tous les documents liés au voyage, par exemple les copies de passeport, les demandes de visa, les feuilles de route contenant les horaires de voyage des professionnels de santé, soient détruits dès que la réunion a eu lieu et que les investigateurs ont été indemnisés pour leurs dépenses, afin que leurs données à caractère personnel ne soient pas conservées inutilement et donc exposées à une utilisation ou à une divulgation non autorisée.

3.3.d La CRO exige des Sous-traitants dont les applications/logiciels sont utilisés, qu'ils mettent en œuvre des mesures techniques et organisationnelles appropriées par rapport au risque présenté par l'activité de traitement, et en particulier que les outils disposent de contrôles appropriés pour limiter l'accès aux seules personnes qui sont autorisées à traiter les données à caractère personnel. Conformément à l'article 29 du RGPD, toute personne ayant accès à des données à caractère personnel, ne traite ces données que sur instructions du responsable du traitement, à moins que le droit de l'Union ou d'un État membre ne l'exige.

Exemple :

- La CRO fait appel à un fournisseur qui héberge l'eTMF et s'arrange avec lui pour que le personnel du fournisseur n'ait pas accès aux données stockées de l'étude, y compris les données à caractère personnel, mais accède uniquement aux informations du compte d'utilisateur du personnel de la CRO pour l'aider à résoudre les problèmes techniques.

3.4 Précision

Cette section fait référence à l'article 5 du RGPD, qui stipule que *" les données à caractère personnel sont : .... c)* ***exactes et, si nécessaire, mises à jour ;*** *toutes les mesures raisonnables sont prises pour que les données à caractère personnel inexactes, au regard des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans délai (****exactitude****) ; "*

Une CRO fournissant des services pour la recherche clinique doit être en mesure de démontrer, par le biais de ses politiques et de ses formulaires de saisie des données, comment elle a intégré la vérification de la qualité des données dans les services qu'elle fournit aux promoteurs. La CRO conservera des enregistrements dans le dossier de l'étude, mettra en œuvre et suivra les instructions du Promoteur pour les processus concernés.

Domaine d'application. Les exigences de la présente section s'appliquent aux CRO qui fournissent un ou plusieurs des services suivants énumérés à l'annexe 2 et figurant dans le document 02 :

- (3) Sélection du site et contrat
- (4) Collecte des données
- (5) Contrôle
- (6) Suivi médical
- (7) Pharmacovigilance
- (8) Services directs aux patients
- (9) Gestion des données
- (12) Gestion financière
- (15) Audits
- (16) Fourniture de services de gestion informatique
- (20) Tenue du Trial Master File (TMF)
- (22) Services réglementaires et de mise en place d'études
- (23) Organisation des réunions investigateurs

Exemples :

- Si une CRO est engagée par un promoteur pour plus d'une étude, par exemple l'extension d'une étude, où les professionnels de santé sont invités à participer à l'étude initiale, une bonne pratique consisterait à ce que, pour la nouvelle étude/l'étude d'extension, la CRO demande aux professionnels de santé de confirmer si les CV, les licences médicales et les autres documents nécessaires obtenus précédemment dans le cadre de l'autre étude peuvent être utilisés ou si des versions actualisées sont nécessaires pour les soumissions réglementaires et le TMF.
- Une CRO fournissant un service de faisabilité et de sélection des investigateurs est chargée par le promoteur de créer une base de données de tous les investigateurs sollicités. Cette base de données comprendra également les professionnels de santé qui ont été sélectionnés et engagés, ainsi que ceux qui n'ont pas été sélectionnés et qui n'ont pas été engagés, mais qui peuvent être contactés par le promoteur pour de futures études. La meilleure pratique consisterait à s'assurer que les professionnels de santé connaissent les coordonnées du promoteur pour communiquer les modifications de leurs données ou exercer leurs droits en matière de protection des données et, si la CRO reçoit de telles informations, elle doit les communiquer au promoteur.

Les paragraphes suivants de la section 3.4 visent à garantir l'exactitude des données collectées sur les Personnes concernées par l'étude.

3.4.1 Mise en place de l'étude

L'objectif est de faciliter une Collecte (de données) complète et de minimiser les erreurs de saisie et le risque de déviation des données à caractère personnel.

3.4.1.a La CRO doit mettre en place les outils de collecte de données, y compris la base de données de l'étude et les cahiers d'observations (CRF), de manière à faciliter l'exactitude des données et à pouvoir les vérifier le plus tôt possible au cours du processus de collecte des données.

Voici quelques exemples de types de contrôles à mettre en œuvre : :

- ***Contrôles de validation des données*** pour s'assurer que le cahier d'observations n'autorise que certaines valeurs et entrées et que les variables textuelles non structurées ne sont utilisées que lorsque cela est dûment justifié.

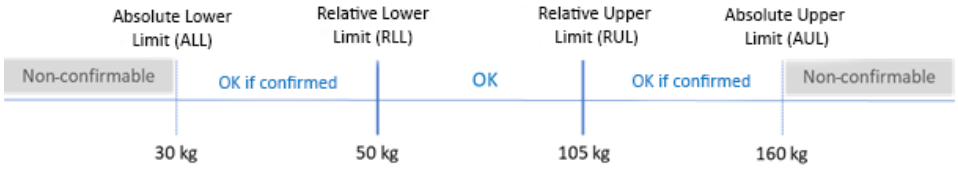
- ***Contrôles de format/type*** pour vérifier que les données sont collectées selon le format/type demandé : format de date, codé, entier, etc...

  Exemple : Une date demandée au format jj-mm-aaaa mais complétée comme suit : 01-19-Mar, est rejetée.

- ***Les contrôles de présence*** permettent de définir si une variable est obligatoire ou non. Il est également possible de notifier l'absence d'une variable mais de confirmer que cette variable n'est pas disponible.

- ***Contrôles de plausibilité*** permettant de vérifier si une valeur se situe ou non dans les limites prévues. Ces contrôles peuvent être définis lors de la configuration de la base de données. Il convient de faire la distinction entre les limites relatives et les limites absolues.

  Exemple pour le poids d'un patient :



- ***Contrôles de cohérence*** visant à détecter les combinaisons de variables impossibles ou improbables.

  Exemple : sexe masculin et patiente ménopausée (combinaison impossible) ; sexe féminin, âge = 50 ans et patiente en âge de procréer (combinaison improbable).

- ***Contrôles des dates*** pour vérifier la chronologie des dates les unes par rapport aux autres.

3.4.2 Supervision de la Collecte (de données à caractère personnel)

3.4.2.1 Collecte (de données) par les professionnels de santé

3.4.2.a La CRO doit documenter les processus mis en œuvre pour garantir l'exactitude pendant la collecte des données, y compris l'identification, les rôles et les capacités des personnes impliquées dans ces processus, afin de vérifier qu'aucune altération n'est possible qui pourrait fausser l'exactitude de la collecte des données. Dans le cas d'une étude utilisant un cahier d'observations électronique (eCRF), la CRO doit s'assurer qu'il existe des mesures de sécurité et des caractéristiques de l'outil eCRF qui mettent en œuvre d'une piste d'audit et des contrôles adéquats pour empêcher l'interception ou la distorsion des données pendant qu'elles sont en transit.

Voici quelques exemples de types de contrôles à mettre en œuvre :

- Dans le cas d'une étude utilisant un cahier d'observations papier, les mesures mises en œuvre pour les processus de gestion du cahier d'observations, telles que les suivantes, doivent être décrites :

  Envoi des documents du cahier d'observations du Site Investigateur de l'étude au bureau de saisie des données :

  - Par voie électronique : numérisation et chargement via une plateforme sécurisée.
  - Envoi des cahiers d'observations papier : recours à une société distributrice de courrier qualifiée et auditée mettant en œuvre des mesures de sécurité adéquates pour l'envoi des cahiers d'observations papier.

- Suivi des CRF reçus et vérification de la réception (par exemple, nombre de CRF reçus par rapport au nombre attendu).
- Saisie des données collectées dans les CRF.
- Gestion des demandes de correction.
- Stockage des CRF papier dans un local sécurisé.

3.4.2.b La CRO doit s'assurer que toutes les mesures visant à garantir l'exactitude sont correctement mises en œuvre pendant toute la durée de l'étude clinique, que cette mise en œuvre est correctement documentée et que cette documentation fait l'objet d'un audit régulier.

Voici quelques exemples de types de contrôles à mettre en œuvre :

- Dans le cas d'un cahier d'observations papier, former les opérateurs de saisie des données de la CRO (formation avec des patients fictifs documentés, utilisation des directives de saisie des données, etc.) et adapter le niveau de saisie des données à l'étude (saisie unique, double saisie avec ou sans adjudication, etc.)
- Veiller à ce que les données à caractère personnel soient collectées au sein du Site Investigateur de l'étude par du personnel qualifié, formé à l'étude et à la législation en vigueur (par exemple, bonnes pratiques cliniques, norme ISO 14155, etc.)
- S'assurer que le personnel chargé de la saisie des données est autorisé à le faire par l'investigateur principal, vérification de la délégation des tâches (le cas échéant).
- Élaborer et fournir au centre les règles de remplissage du cahier d'observations (guide de remplissage du cahier d'observation électronique ou papier, didacticiel vidéo, FAQ, etc.)
- Veiller à ce que les données soient signées par l'investigateur principal pour certifier l'exactitude des données ; signature via le cahier d'observations électronique et/ou signature sur les cahiers d'observations papier avant de geler la base de données.
- Fournir les codes d'accès au cahier d'observation électronique au professionnel de santé uniquement après vérification de sa formation et de sa participation à l'étude.
- Veiller à ce qu'un système d'audit trail soit disponible.
- Veiller à ce que la liste des utilisateurs du cahier d'observation électronique soit régulièrement vérifiée et enregistrée dans le TMF de l'étude.
- Si les exigences relatives à la mise en place de la base de données sont remplies, les données saisies seront vérifiées automatiquement afin de détecter les données manquantes, hors limites et incohérentes, conformément au fichier spécifique des contrôles et au cahier d'observations annoté validé lors de la phase de mise en place de la base de données (voir la section ci-dessus).

3.4.2.2 Collecte de données issues d'autres sources

Cette section s'applique lorsque des données externes (par exemple, des résultats d'analyse d'échantillons biologiques, des données d'imagerie, etc.), y compris les données dites "sources", doivent être intégrées dans la base de données de l'étude. Les données doivent être intégrées de manière à garantir l'exactitude et l'exhaustivité des données à caractère personnel et à les attribuer correctement au bon sujet de l'étude.

> **3.4.2.c** La CRO doit rédiger un document de spécification décrivant toutes les mesures et caractéristiques de la mise en place et des processus de transfert des données externes et de leur intégration dans la base de données de l'étude. Le document de spécification doit être porté à la connaissance de l'expéditeur des données, avant la réception de ces données par la CRO, afin de s'assurer que ces mesures et caractéristiques sont correctement mises en œuvre par l'expéditeur.

Le présent document de spécification détaille, le cas échéant, les éléments suivants :

- Le type de données attendu, le format, la fréquence d'envoi, etc.
- Transferts de données sécurisés de la source vers la CRO : par exemple, protocole SFTP ou HTTPS, ou tout autre processus de transfert sécurisé.
- Procédures de contrôle des données externes reçues avant leur intégration dans la base de données; comment s'assure-t-on que les données reçues sont conformes aux spécifications.

Dans certains cas, les données sont directement téléchargées dans la base de données par le personnel des Sites Investigateurs ou par des fournisseurs externes, par exemple en chargeant des images ou des comptes-rendus d'hospitalisation via le cahier d'observations électronique, etc.

Ces enregistrements ou ensembles de données peuvent à l'origine contenir des Identifiants directs, par exemple le nom et la date de naissance d'une personne concernée.

> **3.4.2.d** La CRO met en œuvre et documente le processus garantissant que les identifiants directs sont supprimés des données de santé des personnes concernées transmises par l'expéditeur avant la réception de ces données par la CRO.

Dans certains cas, par exemple pour des données d'imagerie DICOM, un processus de pseudonymisation, automatique ou manuel, peut être mis en œuvre au moment de leur téléchargement dans le cahier

d'observations électronique. Ce processus doit être correctement documenté conformément aux exigences ci-dessus.

3.4.3 Vérification des données

Domaine d'application. Les exigences de cette sous-section ne s'appliquent que lorsque la CRO supervise la surveillance (voir annexe 2, (5) Monitoring, (6) Monitoring médical, (7) Pharmacovigilance) ou est impliquée dans le data-management (voir annexe 2, (9) Data-management).

3.4.3.a La CRO détaille, dans le plan de surveillance clinique ou dans un document équivalent, tous les processus liés à la vérification de l'exactitude et de l'exhaustivité des données à caractère personnel.

3.4.3.b La CRO doit s'assurer que le personnel chargé de la surveillance est qualifié et connu du promoteur. La CRO doit conserver tous les documents et enregistrements appropriés démontrant que cette exigence est correctement mise en œuvre.

Voici quelques exemples de types de contrôles à mettre en œuvre :

- Les CV des responsables sont régulièrement mis à jour et vérifiés.
- Le personnel responsable a reçu une formation appropriée et dispose d'une attestation de formation sur l'étude.
- Les responsables sont portés à la connaissance du promoteur dans une liste de personnes autorisées.

3.4.3.c La CRO vérifie, par l'intermédiaire du personnel chargé du suivi, l'exactitude et l'exhaustivité des données à caractère personnel conformément aux instructions du promoteur. La CRO envoie les queries auprès du personnel du Site Investigateur dès que possible et veille à ce qu'elles soient résolues.

3.5 Limitation du stockage

Domaine d'application. Les exigences de la présente section s'appliquent à toutes les classes de services de l'annexe 2, à l'exception de (1) Synopsis, protocole et conception du cahier d'observation, (2) Conception du formulaire de consentement éclairé et de la notice d'information et (13) Divulgation publique.

Cette section fait référence à l'article 5 du RGPD, qui stipule que *" les données à caractère personnel sont : .... e)* ***conservées sous une forme permettant l'identification des personnes concernées*** *pendant une durée* ***n'excédant pas celle nécessaire à la réalisation*** *des finalités pour lesquelles elles sont traitées ; les Données à caractère personnel peuvent être stockées pendant une durée plus longue dans la mesure où elles sont traitées uniquement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, sous réserve de la mise en œuvre des mesures techniques et organisationnelles appropriées requises par le présent règlement afin de sauvegarder les droits et libertés de la personne concernée (***" limitation du stockage "***).*

Afin de pouvoir conserver les données à caractère personnel en tant que responsable de la mise en œuvre du traitement, conformément à l'article 89, paragraphe 1, du RGPD, la CRO doit maintenir la conformité avec le présent Code de conduite et en particulier ses garanties pour les droits et libertés des personnes concernées, y compris la minimisation des données et la pseudonymisation, et la CRO doit agir selon les instructions du responsable du traitement.

Pour démontrer qu'elle est responsable de la conservation appropriée des données, une CRO doit inclure des dispositions relatives à la conservation des données et à la limitation du stockage dans l'accord de traitement des données conclu entre le promoteur et la CRO ; elle doit également élaborer les documents attestant du

renvoi au promoteur des documents de l'étude contenant des données à caractère personnel ou de la destruction des données, par exemple les instructions relatives à l'envoi du TMF, les courriers électroniques, les formulaires accusant réception du TMF, les formulaires/certificats de destruction des documents, etc.

Exemples :

- La CRO qui fournit des services de gestion des données (voir la liste des services à l'annexe 2) élabore les spécifications de transfert des données et classe les documents de preuve, y compris la confirmation de la réception des données par le promoteur.
- La CRO qui fournit des services de déclassement (voir la liste des services à l'annexe 2) met en œuvre un contrat régissant le processus de suppression des données et la production de certificats de destruction des données attestant que le service a bien été fourni.
- Le promoteur peut demander l'assistance de la CRO pour les inspections, le traitement à des fins secondaires, etc., c'est pourquoi le promoteur peut demander à la CRO de conserver les données de l'étude clinique après la fin de l'étude clinique ; pendant la durée de conservation, la CRO doit s'assurer qu'elle est en mesure de produire des preuves du niveau de sécurité approprié pour l'archivage, y compris les listes d'accès, la politique de sécurité physique/les normes appliquées pour les zones de stockage, etc.

3.5.a La CRO tient des registres documentant les instructions du responsable du traitement en ce qui concerne les durées de conservation des données.

3.5.b La CRO met en œuvre la durée de conservation déterminée aux données qu'elle traite sur les instructions du responsable du traitement, à moins qu'une loi applicable de l'Union ou d'un État membre n'exige la conservation des données à caractère personnel.

3.5.c La CRO doit se conformer au présent Code de conduite pendant toute la durée de conservation des données.

3.5.d La CRO veille à ce que, lorsque des données sont conservées dans des archives, les mesures techniques et organisationnelles mises en œuvre pour protéger ces données archivées soient adaptées aux risques spécifiques pour les droits des personnes concernées et, sauf justification contraire, bénéficient au moins du même niveau de protection que les données conservées dans les lieux de stockage autres que les archives.

3.5.e Le respect des mesures techniques et organisationnelles mises en œuvre doit être maintenu pendant toute la durée de vie des données archivées et la conformité des archives doit être vérifiée et re-certifiée à intervalles réguliers.

3.5.f Selon les instructions données par le responsable du traitement, la CRO supprime toutes les données à caractère personnel qui ont atteint la fin de la période de conservation. De plus, la CRO doit mettre en place une procédure de suppression de toutes données existantes restantes pour lesquelles une telle instruction ne peut être identifiée. La destruction ou l'anonymisation des données doit être effectuée conformément aux normes industrielles reconnues et doit être vérifiée pour s'assurer que toutes les données à caractère personnel ont été supprimées ou écrasées en toute sécurité.

3.5.g La CRO examine et identifie régulièrement les données pour lesquelles la durée de conservation a expiré. Ces procédures peuvent être manuelles mais doivent être automatisées lorsque cela est techniquement possible.

Exemple :

- La CRO met en œuvre un outil de recherche de données qui identifie et signale les données pour lesquelles la durée de conservation enregistrée dans les métadonnées s'est écoulée.

3.6 Intégrité et confidentialité

Cette section fait référence à l'article 5 du RGPD, qui stipule que " les *données à caractère personnel sont traitées de manière à assurer une* ***sécurité*** *appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dommages accidentels, à l'aide de mesures techniques ou organisationnelles appropriées* (" intégrité et confidentialité ") ".

Domaine d'application : Les exigences de cette section s'appliquent, conformément au document 02, à toutes les classes de services de l'annexe 2, à l'exception de (1) Synopsis, protocole et conception du cahier d'observations, (2) Conception du formulaire de consentement éclairé et notice d'information et (13) Divulgation publique et (17) Fourniture d'une infrastructure d'hébergement physique.

Pour satisfaire à cette obligation, la CRO doit mettre en œuvre les processus nécessaires pour préserver la confidentialité et l'intégrité des données à caractère personnel des personnes concernées. Pour démontrer sa responsabilité dans la mise en œuvre de ce principe, la CRO doit élaborer une ou plusieurs politiques et veiller à ce que les processus régis par ces politiques fassent l'objet d'un suivi, d'un audit et d'une documentation par le biais des caractéristiques pertinentes des systèmes d'information de la CRO.

3.6.a Une CRO élabore des politiques et des procédures de gestion de la confidentialité, y compris des contrôles appropriés, qui garantiront la confidentialité et l'intégrité des données à caractère personnel, conformément à l'évaluation des risques inhérents au traitement, et doit être en mesure de démontrer la conformité avec les mesures techniques et organisationnelles mises en œuvre. Les mesures techniques et organisationnelles requises pour préserver la confidentialité et l'intégrité des données comprennent au minimum :

A. Contrôles d'accès qui n'accordent l'accès et les autorisations que sur la base du besoin de savoir ("moindre privilège") ;
B. Accéder régulièrement aux revues ;
C. Procédures de traitement et de divulgation des données adaptées au niveau de risque associé à l'activité de traitement ;
D. Formation et sensibilisation du personnel autorisé à traiter les Données à caractère personnel qui couvre les obligations de confidentialité liées à l'activité de traitement ; et
E. Clauses contractuelles de confidentialité conformément au chapitre 2 du présent code.

Exemples :

- La CRO chargée du contrôle (cf liste des services à l'annexe 2) veille à ce que les responsables du traitement signent des contrats de travail comprenant des dispositions relatives aux obligations de confidentialité à l'égard des données à caractère personnel des personnes concernées ; les dossiers de formation des responsables du traitement contiennent des règles interdisant l'extraction de documents sources non pseudonymisés au moment de l'accès direct aux données.
- La CRO assurant le suivi médical, les rapports de sécurité et la pharmacovigilance (cf liste des services à l'annexe 2) classera la correspondance électronique, les rapports et les formulaires d'évaluation des incidents documentant la réponse aux cas d'enregistrements mal pseudonymisés envoyés par erreur par les Sites Investigateurs aux ARCs moniteurs de la CRO dans le cadre des rapports de sécurité, etc.
- La CRO qui fournit des services gérés par les IT, par exemple une plateforme de saisie électronique des données en ligne (cf liste des services à l'annexe 2), intègre dans son produit IT les outils et caractéristiques appropriés pour préserver la sécurité dès que possible au cours de la conception et du développement du produit, et intègre et effectue en permanence des tests pertinents.

- La CRO qui fournit des services directs aux patients (cf liste des services à l'annexe 2) doit organiser le traitement des données en accordant l'accès et les autres autorisations applicables en fonction du besoin de connaître, par exemple en séparant les systèmes et les bases de données utilisés pour traiter les données d'identification des personnes concernées par l'étude dans le cadre du service direct aux patients et ceux destinés au traitement des données pseudonymisées relatives à la santé utilisées pour d'autres services fournis par la CRO pour le compte du promoteur.

3.6.1 Pseudonymisation

La pseudonymisation est utilisée dans la recherche clinique afin de protéger la vie privée et les droits des sujets d'étude. Par défaut, toutes les données traitées par les CRO doivent être pseudonymes et les données d'identification ne doivent être traitées que par exception et conformément à la section 3.6.3. Afin de rendre les ensembles de données pseudonymes, un processus est mis en œuvre pour remplacer les données à caractère directement identifiante des sujets de l'étude par un code d'identification du sujet.

Les ensembles de données pseudonymes peuvent inclure des identifiants indirects mais doivent exclure les identifiants directs. Les données pseudonymes restent des données à caractère personnel.

- Les identifiants directs peuvent être utilisés pour identifier une personne sans informations supplémentaires ou par recoupement avec d'autres informations qui sont dans le domaine public.

  Il est conseillé de traiter d'autres informations individualisées telles que les numéros de dossier médical et les numéros de téléphone comme des identifiants directs, même si des informations supplémentaires sont nécessaires pour les relier à une identité, parce que ces formes d'identification sont largement utilisées et donc disponibles pour être reliées à des identités.

  Voici quelques exemples d'identifiants directs :

  Nom, adresse, numéro de téléphone, adresses électroniques et autres numéros d'identification uniques, caractéristiques ou codes comme le numéro d'immatriculation du véhicule, le numéro de sécurité sociale (NIR), les photographies de signes distinctifs et les données biométriques (telles que définies par le RGPD).

- Les identifiants indirects sont des données qui, en elles-mêmes, ne permettent pas d'identifier une Personne spécifique, mais qui peuvent être agrégées et mises en relation avec d'autres informations pour identifier les personnes concernées.

  Le code d'identification du sujet qui peut être utilisé pour la pseudonymisation est un identifiant indirect.

  Voici d'autres exemples d'Identifiants indirects :

  Sexe, date de naissance ou âge, lieux géographiques (tels que codes postaux, géographie de recensement, informations sur la proximité de points de repère connus ou uniques), adresse IP, langue parlée à la maison, origine ethnique, nombre total d'années de scolarité, statut marital, antécédents criminels, revenu total, appartenance à une minorité visible, profession, dates des événements, nombre d'enfants, diagnostics et procédures de haut niveau.

Remarque :

Si une CRO fournit un service au responsable du traitement qui implique la génération de codes d'identification des sujets, par exemple dans le cadre de la fonctionnalité d'un système IWRS exploité par une CRO, la CRO doit s'assurer que les codes excluent les identifiants des sujets de l'étude tels que le numéro d'identification national ou d'assurance, les initiales, la date de naissance ou l'âge. La CRO doit s'assurer que les codes sont suffisamment robustes en tant que méthode de pseudonymisation et qu'ils présentent une séquence aléatoire de symboles sans modèle reconnaissable au sein d'une étude qui pourrait poser un risque de réidentification. La CRO doit prendre en considération le risque de réidentification et doit s'assurer de choisir les techniques appropriées pour réduire ce risque.

Remarque :

Les numéros d'appareils peuvent, dans certains cas d'utilisation, constituer un «Identifiant direct». En tant que tels, ils doivent être traités au cas par cas, en tenant compte de leur utilisation et de leur potentiel/risque de réidentification.

3.6.1.a Une CRO traite les données à caractère personnel des sujets de l'étude uniquement sous forme de pseudonyme, à moins que le traitement d'identifiants directs ne soit strictement nécessaire à la fourniture des services et qu'il soit effectué sur instruction du responsable du traitement dans le respect du principe de minimisation des données.

Exemples :

Le traitement d'identifiants directs par une CRO peut être justifié dans les cas suivants :

- La CRO est engagée par le promoteur pour la prestation de services directs aux patients (cf liste des services à l'annexe 2, classe (8)) traite les identifiants directs parce que la réalisation de l'objectif est impossible sans l'accès à ces données.
- Les moniteurs et les auditeurs internes de la CRO (cf liste des services à l'annexe 2, classes (5), (15)) auront accès aux registres d'identification des sujets de l'étude/ registres des patients, notamment pour vérifier le processus de consentement et la cohérence du remplissage des cahiers d'observation à partir des données sources.

3.6.2 Anonymisation

Il peut être souhaitable de traiter un ensemble de données en dehors du Protocole de recherche, ce qui peut être possible à condition que les données soient anonymisées. L'avis du groupe de travail Art. 29[10] auquel se réfère la ligne directrice de l'Agence européenne des médicaments (EMA)[11] , et toute version actualisée de ces lignes directrices, fixe un seuil élevé pour parvenir à l'anonymisation. Les données sont considérées comme anonymes lorsqu'elles sont rendues sous une forme qui ne permet pas d'identifier les personnes et que l'identification par "*tous les moyens susceptibles d'être raisonnablement mis en œuvre*" par le responsable du traitement ou par un tiers, y compris la combinaison des données avec d'autres données, n'est pas susceptible d'avoir lieu.

Une CRO peut proposer l'anonymisation en tant que service. Elle doit documenter le processus d'anonymisation et fournir une assistance au responsable du traitement dans la définition des paramètres et l'évaluation des risques de réidentification sur le jeu de données résultant.

Remarque :

La CRO applique des méthodes d'anonymisation conformes aux normes reconnues et/ou fondées sur les orientations et les recommandations du Comité européen de la protection des données, des autorités nationales de contrôle de la protection des données et des autorités de contrôle régissant le domaine de la recherche clinique, par exemple l'EMA.

3.6.2.a Une CRO fournissant l'anonymisation en tant que service doit disposer d'un personnel expérimenté dans l'analyse des données, capable d'effectuer une analyse du risque de réidentification afin de démontrer au promoteur qu'un ensemble de données est anonyme.

3.6.3 Traitement des données à caractère personnel directement et indirectement identifiantes des sujets de l'étude

Le personnel de la CRO peut recevoir ou accéder à des données à caractère personnel permettant d'identifier directement ou indirectement les sujets de l'étude aux fins suivantes :

(1) Contrôler et garantir la fiabilité des données de l'étude clinique en vérifiant que l'investigateur transfère les données des dossiers médicaux vers les CRF avec précision et exactitude. La CRO ne transfère pas ces données dans ses systèmes informatiques en vue d'un traitement ultérieur, de sorte que l'obligation pertinente de la CRO consiste à se conformer à l'exigence 2.6.a et 2.6.b du présent Code ; toutefois, dans les cas où la CRO traite les données à caractère personnel dans ses systèmes informatiques, par exemple pour la vérification à distance des données sources, les dispositions supplémentaires de la présente section 3.6.3 s'appliquent également.

(2) Fournir des services supplémentaires, qui nécessiteront le traitement des données à caractère personnel directement identifiantes des sujets de l'étude, par exemple le nom, l'adresse postale, les coordonnées électroniques et téléphoniques, les coordonnées bancaires, etc. avec une séparation complète des données pseudonymisées concernant la santé des sujets d'étude.

Exemples :

- Une CRO fournit des services de transport, y compris des transports spéciaux ; l'organisation de voyages, y compris les réservations d'avion, de train, de taxi, d'hébergement.

[10] Avis 05/2014 du groupe de travail "Article 29" sur les techniques d'anonymisation (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf) ou toute version ultérieure de celui-ci.

[11] Orientations externes de l'EMA sur la mise en œuvre de la politique 0070 de 2019 (https://www.ema.europa.eu/en/documents/other/european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use_en.pdf)

- Une CRO fournit des produits électroniques permettant une interaction directe avec le patient via des plateformes en ligne ou des systèmes de messagerie électronique, y compris des résultats électroniques enregistrés par le patient (ePRO) ou permettant aux patients de donner leur consentement électronique pour participer à l'étude (eConsentement), etc.
- Une CRO aide le promoteur à répondre aux demandes et aux droits des personnes concernées.
- Une CRO fournit des services de suivi au promoteur et doit consulter les documents sources contenant des identifiants directs. D'ordinaire, lorsque le suivi est effectué, il n'y a pas de transmission de données à caractère personnel identifiables aux systèmes informatiques de la CRO, mais dans les cas où il y a un traitement dans les systèmes informatiques de la CRO de données à caractère personnel identifiables à des fins de vérification des données sources à distance, la CRO doit se référer et se conformer à toutes les lignes directrices européennes et nationales applicables sur le suivi à distance, telles que le document de recommandation sur les éléments décentralisés dans les essais cliniques par l'EMA, Version 01, 13 décembre 2022.
- Les représentants des groupes/organisations de défense des patients communiquent en face à face avec les sujets de l'étude et leur famille afin de comprendre, de partager des informations avec la communauté de la recherche clinique/les parties prenantes et de répondre aux préoccupations et aux difficultés rencontrées par les sujets de l'étude au cours de leur participation à l'étude.

3.6.3.a Une CRO doit disposer de procédures lui permettant d'aider le responsable du traitement à définir les données à caractère personnel minimales nécessaires des Personnes concernées par l'étude pour que la CRO puisse fournir les services qui requièrent l'accès de la CRO à la fois aux identifiants directs et aux données pseudonymisées des Personnes concernées par l'étude.

3.6.3.b Lors du traitement de données à caractère personnel directement identifiables, la CRO met en œuvre des mesures de sécurité techniques et organisationnelles supérieures appropriées, conformément aux lignes directrices européennes et nationales applicables[12] , afin de garantir le maintien de la confidentialité des données à caractère personnel des sujets de l'étude.

Notes sur les mesures techniques et organisationnelles supérieures :

- La CRO peut confier le traitement des Identifiants directs à un sous-traitant qui aura une interaction directe avec les sujets de l'étude. La CRO doit recevoir des documents de responsabilité de la part de ces fournisseurs. La CRO doit s'assurer que les preuves de prestation de services, par exemple les factures, ne contiennent pas d'identifiants directs des sujets de l'étude susceptibles d'accroître le risque d'annulation de la pseudonymisation.
- Les CRO qui traitent les identifiants directs elles-mêmes ainsi que les données pseudonymes doivent appliquer des mesures techniques et organisationnelles supplémentaires consistant en des normes plus élevées de séparation des données, de contrôle d'accès et de transparence sur le traitement. Ces mesures visent à empêcher la combinaison de données directement identifiantes avec des données pseudonymisées, ainsi que les risques associés d'inversion involontaire de la pseudonymisation[13].

  Ces mesures visent à garantir ce qui suit :

  1) Ségrégation entre les systèmes et les bases de données utilisés pour traiter les données à caractère personnel directement identifiantes et les ensembles de données pseudonymes via :
     - Contrôle de l'accès aux sites, systèmes et bases de données contenant des données directement identifiantes des personnes concernées par l'étude, de manière à ce que ces données ne soient pas exposées par inadvertance à du personnel non autorisé.
     - Contrôle du personnel, à savoir empêcher que le personnel chargé de traiter des données directement identifiantes ne participe à la fourniture des services en utilisant des données pseudonymes et vice-versa.
     - Empêcher le personnel de combiner des informations provenant de différentes sources pour associer des personnes à l'étude, par exemple en ne faisant appel qu'à un nombre minimal de membres du personnel ou de contractants pour traiter les données d'identification directe des sujets de l'étude ; le personnel chargé de traiter les données d'identification des sujets de l'étude ne sera pas membre d'une équipe projet chargée de superviser l'étude clinique.
     - Contrôle de la communication, à savoir via le Site Investigateur et non avec les patients directement dans la mesure du possible, et lorsque les services nécessitent une communication directe avec les sujets de l'étude, la CRO doit

[12] Document de recommandation sur les éléments décentralisés dans les essais cliniques par l'EMA, Version 01, 13 décembre 2022
[13] Avis n° 5/2014 du groupe de travail «Article 29» sur les techniques d'anonymisation ou toute version ultérieure de celui-ci

minimiser la collecte de données et utiliser des identifiants tokenisés pour les sujets de l'étude dans la mesure du possible.

- Contrôle contractuel, à savoir l'inclusion de dispositions spécifiques dans l'accord de confidentialité avec le personnel affecté ; dispositions spécifiant les divulgations autorisées.

2) La CRO fournit suffisamment d'informations sur les méthodes de traitement au commanditaire lorsque la CRO traite à la fois des données directement identifiantes et des données pseudonymes pour que le promoteur puisse s'assurer que les personnes concernées par l'étude sont pleinement informées à l'avance des conditions de traitement des données, comme l'exige la législation applicable en matière de protection des données.

3) La CRO dispose de processus et de documents appropriés pour démontrer qu'elle est responsable de leur mise en œuvre, y compris des registres de traitement, spécifiques à la réalisation de ces tâches. Tous ces documents sont révisés en temps utile et conservés en toute sécurité.

4 Obligations de la CRO en tant que sous-traitant

La CRO s'engage envers le promoteur à remplir ses obligations en tant que sous-traitant afin de garantir le traitement licite et équitable des données à caractère personnel. Cela permet de garantir le maintien des droits et libertés des personnes concernées.

Les principales obligations de la CRO sont les suivantes (le cas échéant) :

- Désignation d'un délégué à la protection des données à caractère personnel
- Mise en place et maintient de mesures techniques et organisationnelles (MTO) appropriées
- Enregistrement des données requises pour le traitement des données
- Gestion et audit des sous-traitants
- Assistance et collaboration avec les responsables du traitement
- Transferts de données vers des pays tiers

Domaine d'application : Les exigences expliquées dans chaque section du présent chapitre s'appliquent de manière générale, c'est-à-dire à toutes les classes de services énumérées à l'annexe 2, à l'exception des classes (1) et (2).

4.1 Désignation d'un DPD

Article 37 RGPD : une désignation de DPD doit avoir lieu lorsque *" les activités de base du responsable du traitement ou du sous-traitant consistent à traiter à grande échelle des catégories particulières de données conformément à l'article 9 et des données à caractère personnel relatives aux condamnations pénales et aux infractions visées à l'article 10. "*

Un délégué à la protection des données à caractère personnel (DPD) doit être désigné par la CRO lorsque le RGPD l'exige. Étant donné que les CRO, indépendamment du nombre de leurs employés et de leur taille, traitent des données de santé, qui constituent une catégorie particulière de données à caractère personnel, le plus souvent à grande échelle, il est très probable qu'un DPD doive être désigné par les CRO.

Exemple :

- Une CRO qui ne compte qu'un petit nombre d'employés devra probablement désigner un DPD externe afin d'éviter un conflit d'intérêts entre un rôle opérationnel et le poste de DPD.

Une CRO peut également être tenue de désigner un DPD en cas de "*suivi régulier et systématique des personnes concernées à grande échelle*", par exemple lorsque des dispositifs portables sont utilisés dans le cadre de l'étude pour surveiller l'état de santé des sujets de l'étude. La CRO doit suivre les orientations fournies par l'autorité compétente en matière de protection des données et les lignes directrices du Comité européen de protection des données pour déterminer si elle doit désigner un DPD.

Il est important de noter qu'il appartient à la CRO de déterminer si un DPD est requis. Indépendamment de l'applicabilité de la désignation obligatoire, les CRO sont encouragées à désigner un DPD sur la base du volontariat. Le retour d'information du promoteur peut être pris en compte, mais il ne doit pas être le facteur déterminant. Dans le cas où une CRO estime qu'elle n'a pas besoin d'un DPD et motive dûment ce choix de ne pas en désigner un, d'autres mécanismes permettant d'assurer la Conformité au RGPD doivent être adoptés. Les fonctions normalement exercées par le DPD devraient être assurées en interne malgré l'absence de DPD ; par exemple, des processus internes devraient être mis en place pour que les activités de traitement soient dûment contrôlées et enregistrées, que des évaluations des risques soient effectuées si nécessaire, qu'un point de contact soit identifié pour aider à traiter les demandes et les droits des personnes concernées, qu'une formation adéquate sur la conformité au RGPD soit dispensée aux employés, qu'un point de contact soit identifié pour assurer la liaison avec les Autorités de contrôle, etc.

Le délégué à la protection des données d'une CRO ne doit pas également agir en tant que délégué à la protection des données du promoteur, compte tenu du risque de conflit d'intérêts.

Exemple :

- Le responsable du traitement a l'obligation de contrôler la Conformité du traitement des données par le sous-traitant. Si le délégué à la protection des données de la CRO agit en tant que délégué à la protection des données du promoteur

(responsable du traitement), il contrôlera le traitement des données du promoteur et de la CRO (sous-traitant). Le DPD peut être confronté à un défi lorsqu'il contrôle le traitement des données de la CRO et qu'il détecte un cas de non-conformité de la part de la CRO. Le DPD serait placé dans une position où son objectivité est sujette à caution, et il pourrait éprouver des difficultés à agir dans l'intérêt du sponsor lorsque cela peut nécessiter d'agir au détriment de la CRO qui l'emploie.

4.1.a La CRO désigne un DPD pour son organisation si l'exigence de l'article 37 du RGPD est remplie. Si un DPD n'est pas désigné, la CRO doit documenter les raisons pour lesquelles un DPD n'a pas été désigné et quel soutien est fourni à la place d'un DPD pour se conformer au RGPD.

4.1.b La CRO désigne un DPD sur la base de ses qualifications et de sa capacité à exécuter les tâches prévues par le RGPD. La CRO n'interfère pas dans l'exécution par le DPD des tâches qui lui incombent en vertu du RGPD.

4.1.c La CRO soutient le DPD dans l'accomplissement de ses tâches en lui fournissant les ressources nécessaires et en l'impliquant en temps utile dans les questions relatives à la protection des données.

4.1.d Les CRO doivent faire en sorte que le DPD rende compte à la direction générale de leur organisation.

4.1.e La CRO veille à ce que les coordonnées du DPD figurent dans les registres de traitement et soient facilement accessibles par le biais de leur avis de confidentialité au sein de leur organisation, aux personnes concernées, ainsi qu'aux promoteurs et aux autorités de contrôle, le cas échéant.

4.2 Mesures techniques et organisationnelles (MTO)

Cette section précise les exigences relatives à la mise en œuvre des mesures techniques et organisationnelles visant à garantir et à pouvoir démontrer que le traitement est effectué conformément à l'article 32 du RGPD "Sécurité du traitement" ;

> *" [...] le responsable du traitement et le sous-traitant mettent en œuvre les **mesures techniques et organisationnelles appropriées** pour assurer un niveau de **sécurité adapté au risque** [...]*
>
> ***L'adhésion à un Code de conduite approuvé [...]** ou à un mécanisme de certification approuvé [...] peut être utilisée comme élément permettant de démontrer la conformité aux exigences énoncées dans [...] le présent article."*

Conformément aux exigences du RGPD, tant le responsable du traitement que le sous-traitant (et donc les CRO) doivent mettre en œuvre des mesures organisationnelles et techniques pour garantir un niveau de sécurité approprié au regard des risques associés aux données traitées.

Un Système Management Sécurité de l'Information (SMSI) est une approche systématique composée de processus, de technologies et de personnes qui aide à protéger et à gérer les informations d'une organisation par le biais d'une gestion efficace des risques. Un SMSI contribue à la conformité avec les exigences de l'article 32 du RGPD, selon lesquelles une CRO doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque. Cependant, la mise en œuvre d'un SMSI, à elle seule, ne suffit pas à garantir le respect de l'article 32 du RGPD. Pour être conforme, la CRO doit mettre en œuvre toutes les mesures applicables du Code conformément à sa déclaration d'applicabilité.

Les mesures de sécurité sont sélectionnées en fonction de l'état de l'art et des coûts de mise en œuvre. Les mesures tiennent compte du contexte du traitement, de la nature des données traitées et de la portée du traitement. La probabilité du risque et la gravité pour les droits et libertés des personnes concernées doivent être prises en compte pour sélectionner les mesures organisationnelles et techniques appropriées. Une CRO adhérant au présent Code de conduite doit disposer d'un Système de Management de la Sécurité de l'Information (SMSI) opérationnel conforme aux exigences spécifiées et énumérées dans le document 02 du Code, dont le titre est "Objectifs et exigences en matière de sécurité".

Remarque :

- La plupart des CRO disposent d'un système de gestion de la qualité (SMQ) et, très souvent, ce SMQ fait partie d'une certification ISO 9001. Dans un certain nombre de cas, il peut suffire de compléter le SMQ par des mesures de sécurité de l'information appropriées pour obtenir un SMSI permettant d'adhérer au code.

Les exigences spécifiées dans le document 02 sont des contrôles dérivés des normes existantes suivantes :

1. ISO/IEC 27001 : mai 2017[14] , Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences ;
2. ISO/IEC 27701 : Août 2018, Techniques de sécurité - Extension des normes ISO/CEI 27001 et ISO/CEI 27002 pour la gestion des informations relatives à la vie privée - Exigences et lignes directrices.

Pour toutes les classes de services, la **certification sur la norme ISO 27001 n'est pas exigée** mais constitue une condition favorable à l'adhésion.

Domaine d'application : Les exigences de cette section s'appliquent à toutes les classes de services énumérées à l'annexe 2, et telles que développées et spécifiées dans le document 02 du Code.

4.2.a La CRO établit, met en œuvre, maintient et améliore en permanence un système de gestion de la sécurité de l'information conforme à la méthodologie illustrée par la norme ISO 27001 ou tout autre cadre de conformité équivalent. En d'autres termes, la CRO doit :

- Mettre en œuvre une méthodologie d'analyse des risques afin d'évaluer les risques ;
- Mettre en œuvre des politiques de sécurité ;
- Mettre en œuvre des contrôles de sécurité pour réduire le risque identifié ;
- Évaluer la performance de chaque contrôle mis en place ; et
- Assurer une action corrective et préventive afin d'améliorer la performance des mesures de sécurité.

Le champ d'application du SMSI doit être clairement identifié. Chaque élément sortant du champ d'application doit être clairement documenté.

4.2.b Une CRO adhérant au présent Code doit mettre en œuvre les exigences de contrôle énumérées dans le Document 02 du présent Code qui s'appliquent aux classes de service que le CRO énumère dans sa déclaration d'applicabilité.

4.2.c Tous les documents du SMSI doivent être classés par version et les mécanismes de conservation des versions obsolètes doivent être documentés.

4.2.d Les exigences découlant de la déclaration d'applicabilité de la CRO qui concernent la sécurité de l'information sont toutes couvertes par le SMSI de cette même CRO.

Pour se conformer aux exigences de sécurité du code, la CRO doit poursuivre plusieurs objectifs de sécurité qui doivent être détaillés dans le SMSI de l'organisation, lequel doit être cohérent avec la déclaration d'applicabilité de la CRO.

Toute exclusion d'un contrôle spécifique du SMSI doit être dûment documentée et justifiée au regard des services offerts par la CRO.

[14] Pour éviter toute ambiguïté, la norme ISO 27001:2022 est compatible avec le présent code et les exigences peuvent être lues en conséquence.

4.2.e. Toute exclusion d'une exigence de contrôle découlant de la déclaration d'applicabilité doit être énumérée et justifiée.

4.3 Registres des activités de traitement

La CRO doit tenir des registres des activités de traitement, comme indiqué à l'article 30 du RGPD. Les CRO utilisent souvent des applications et des outils dédiés à la recherche, aux études et à l'évaluation. Les promoteurs peuvent également s'appuyer sur ces outils d'application et sur la tenue de leurs propres registres. Les CRO doivent être en mesure de démontrer la disponibilité de ces registres de traitement pertinents pour les services fournis par la CRO.

Il est important de noter que les exigences relatives aux dossiers de la CRO ne sont pas les mêmes que celles qui s'appliquent au rôle du promoteur en tant que responsable du traitement des données. Le code fait référence à des registres limités aux activités de traitement effectuées en tant que sous-traitant pour le compte du promoteur (responsable du traitement). Les enregistrements de la CRO relatifs au traitement des données sont distincts de ceux exigés du promoteur (responsable du traitement).

Domaine d'application : Les exigences expliquées dans chaque section du présent chapitre s'appliquent de manière générale, c'est-à-dire à toutes les classes de services énumérées à l'annexe 2, à l'exception des classes (1) et (2).

4.3.a La CRO tient un registre des activités de traitement relevant de son contrôle. La CRO est libre de définir le format, pour autant que le rapport comprenne les éléments définis à l'article 30, paragraphe 2.

4.3.b La CRO établit, conjointement avec le responsable du traitement, le processus permettant de fournir à l'autorité de contrôle, sur demande et dans les meilleurs délais, les relevés de traitement.

4.4 Gestion et audit des sous-traitants

Lorsque la CRO conclut un accord contractuel avec des fournisseurs engagés en tant que sous-traitants secondaires, ces contrats sont soumis aux sections 2.4, 2.5, 2.6 et 2.7 du présent Code de conduite. En ce qui concerne les fournisseurs engagés directement par la CRO, il incombe à cette dernière de veiller à ce que les sous-traitants engagés pour traiter les données à caractère personnel pour le compte du promoteur mettent en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données à caractère personnel et agissent conformément aux instructions du promoteur. La CRO est responsable de la performance des sous-traitants engagés au sens de l'article 28, paragraphe 4, du RGPD.

Le promoteur (responsable du traitement) délègue généralement à la CRO le soin de sélectionner les sous-traitants appropriés. Bien que le promoteur puisse déléguer la sélection et l'engagement des fournisseurs en tant que sous-traitants, la CRO doit engager ses sous-traitants conformément à la section 2.5 du présent Code de conduite, et maintenir le promoteur engagé, le cas échéant, tout au long de ce processus. Le processus de sélection doit prendre en considération les compétences et les capacités de conformité du sous-traitant, à savoir sa capacité et son engagement à fournir des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement des données à caractère personnel qui lui sont confiées réponde aux exigences du RGPD.

Domaine d'application : Les exigences expliquées dans chaque section de ce chapitre s'appliquent de manière générale, c'est-à-dire à toutes les classes de services énumérées à l'annexe 2, à l'exception des classes (1) et (2).

4.4.a La CRO doit disposer de procédures définies pour l'approbation, la gestion et la suppression des sous-traitants.

4.4.b Lors de la sélection des sous-traitants ultérieurs, une CRO utilise son expertise pour mener un processus de sélection qui garantira que la CRO ne sélectionne que des sous-traitants ultérieurs qui seront en mesure de fournir les mêmes mesures techniques et organisationnelles que celles que la CRO est tenue de fournir dans le contrat sur le traitement des données.

4.4.c Lorsque la CRO exerce sa diligence raisonnable et son contrôle par le biais d'un audit des sous-traitants secondaires, l'audit est réalisé par un auditeur qualifié et expérimenté qui suit un plan d'audit défini en matière de protection de la vie privée.

4.4.d La CRO contrôle régulièrement la conformité et l'efficacité des mesures techniques et organisationnelles du sous-traitant ultérieur.

4.4.e La CRO signale au responsable du traitement tout problème de non-conformité important et non résolu avec un sous-traitant ultérieur.

Exemple

- Un promoteur a demandé à une CRO d'engager un fournisseur spécifique en tant que sous-traitant. C'est la CRO, et non le promoteur, qui est chargée de la relation contractuelle avec le sous-traitant. Au cours des négociations, le sous-traitant refuse d'incorporer les mêmes conditions de traitement que celles imposées par le commanditaire à la CRO.

  Le promoteur demande à la CRO de tenir compte des préférences du sous-traitant secondaire en ce qui concerne les MTO. La CRO procède à un audit du sous-traitant ultérieur afin de déterminer si les MTO du sous-traitant ultérieur offriront les mêmes niveaux de protection des données que les MTO prévues dans le contrat de la CRO avec le promoteur.

4.5 Assistance et collaboration avec le responsable du traitement

Domaine d'application : Les exigences expliquées dans chaque section du présent chapitre s'appliquent de manière générale, c'est-à-dire à toutes les classes de services énumérées à l'annexe 2, à l'exception des classes (1) et (2).

4.5.1 Fourniture de conseils sur les questions de protection des données de la recherche clinique à un promoteur

Une CRO peut conseiller le promoteur sur les questions de protection des données de la recherche clinique, mais elle ne doit à aucun moment être en mesure de prendre des décisions sur ces questions.

Toutefois, si la CRO estime que le promoteur (responsable du traitement) n'est pas aligné sur le RGPD, elle en informe immédiatement le promoteur et peut lui fournir des conseils sur ce qui, à son avis, permettrait au promoteur (responsable du traitement) de s'aligner sur le RGPD.

4.5.1.a La CRO informe le promoteur si, de l'avis de la CRO, une instruction du promoteur enfreint le RGPD ou d'autres dispositions de l'Union ou de l'État membre en matière de protection des données à caractère personnel.

La CRO peut partager ses idées et ses observations, mais le promoteur doit s'en remettre à son propre DPD ou à son expert en matière de protection de la vie privée pour la décision finale concernant sa réponse à la notification de la CRO.

4.5.2 La CRO en tant que représentant du promoteur lui-même responsable du traitement en vertu de l'article 27

L'article 27 du RGPD s'applique lorsqu'un responsable du traitement (promoteur) n'est pas établi dans l'Union européenne alors que le traitement concerne des données à caractère personnel de personnes de l'UE.

Souvent, dans le domaine de la recherche clinique, le promoteur n'a pas de présence légale ou physique dans l'UE. Toutefois, lors de la définition de l'applicabilité de l'article 27 du RGPD, il convient de noter que le facteur déterminant n'est pas la forme juridique des arrangements de l'entreprise, c'est-à-dire la question de savoir si l'entreprise a constitué une succursale ou une filiale légale, mais plutôt qu'un établissement implique l'exercice effectif et réel d'une activité par le biais d'arrangements stables, conformément au considérant 22 du RGPD.

Il peut y avoir des circonstances dans lesquelles le promoteur demande à la CRO d'intervenir en tant que son représentant. Conformément à l'avis exprimé par le Conseil européen de la protection des données dans les orientations sur l'applicabilité territoriale du RGPD[15] , une CRO ne doit pas agir en tant que Sous-traitant et Représentant pour le même promoteur, en raison d'un éventuel conflit d'obligations et d'intérêts qui pourrait survenir en cas de procédure d'exécution. Cela n'empêche pas une CRO d'assumer le rôle de représentant d'un promoteur pour lequel il n'agit pas en tant que responsable de la mise en œuvre du traitement.

> **4.5.2.a** Une CRO n'agit en tant que représentant de l'UE pour la protection des données d'un promoteur qu'à la condition qu'elle n'agisse pas en même temps en tant que sous-traitant de données pour toute recherche clinique de ce promoteur.

4.5.3 Evaluation de l'impact sur la protection des données à caractère personnel

Le promoteur, en tant que responsable du traitement des données, est également tenu de procéder à une évaluation de l'impact sur la protection des données de toute opération de traitement envisagée de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. La CRO, en tant que sous-traitant des données, n'est pas tenu d'avoir entrepris elle-même une telle évaluation sur les activités de traitement qu'elle effectue, mais elle est tenue d'aider le promoteur à entreprendre cette évaluation.

> **4.5.3.a** À la demande du promoteur, la CRO l'aide à réaliser une analyse d'impact sur la protection des données dans les limites des services qu'elle fournit en vertu du contrat de services et du contrat relatif au traitement des données.

4.5.4 Demandes des Personnes concernées

Le promoteur et la CRO travaillent tous deux avec des données pseudonymisées concernant la santé des sujets de l'étude et des données à caractère personnel identifiables des Professionnels de santé. Lorsqu'elle répond à une demande d'une personne concernée émanant d'un professionnel de santé, la CRO doit s'assurer qu'elle a mis en place des processus permettant de remplir les obligations élaborées dans le contrat relatif au traitement des données, conformément à l'exigence 2.4.g du présent Code.

Si les données pseudonymisées restent des données à caractère personnel, elles ne sont pas directement attribuables à une personne concernée spécifique. Les sites Investigateur de l'étude peuvent être le principal site où les demandes des personnes concernées peuvent être exercées. Dans la mesure où il n'est pas incompatible avec le fait que la CRO ne traite que des données pseudonymes, la CRO doit aider le promoteur à répondre aux demandes des personnes concernées, par exemple en contribuant à faciliter l'exercice de ces droits en relayant les instructions du promoteur sur le site de l'étude. Il peut être demandé à la CRO d'apporter la preuve qu'elle dispose d'une procédure permettant d'exécuter les demandes des personnes concernées en temps utile. Cette preuve peut prendre la forme d'une description des processus, des procédures et d'autres documents qui rendent compte des mesures, des indicateurs clés de performance et du suivi.

[15] Lignes directrices 3/2018 du CEPD sur le champ d'application territorial du RGPD (article 3) Version 2.1 12 novembre 2019

4.5.4.a Une CRO, en accord avec le promoteur, établit et documente un processus de communication avec le promoteur dans le but d'aider ce dernier à répondre aux demandes des personnes concernées dans le cas où un sujet de l'étude contacte directement la CRO.

Exemples :

- Les personnes concernées par l'étude doivent toujours avoir la possibilité de contacter directement le responsable du traitement. Toutefois, étant donné que le promoteur et la CRO ne reçoivent normalement pas de données permettant d'identifier les sujets de l'étude afin de préserver la confidentialité de leur participation et la nature (potentiellement) en aveugle de l'étude, la CRO peut proposer au promoteur de faire en sorte que les sujets de l'étude soient invités à adresser leurs demandes au professionnel de santé qui facilitera l'exercice de leurs droits en tant que sujets de données. Le droit du sujet de l'étude de contacter directement le promoteur doit toujours être réservé, quelles que soient les autres dispositions prises.

  En règle générale, cette recommandation sera communiquée aux sujets de l'étude par le biais du formulaire de consentement éclairé ou d'une notice distincte. Le professionnel de santé doit être chargé d'informer la CRO et/ou le promoteur d'une demande de la personne concernée et de demander des instructions au promoteur/à la CRO sur la manière de traiter la demande.

- Sauf si la CRO fournit un service direct aux patients (cf liste des services à l'annexe 2, classe (8)), les sujets de l'étude ne reçoivent normalement pas les coordonnées du responsable du traitement des données pour l'exercice des demandes des sujets de l'étude. Toutefois, si la CRO et le promoteur en décident autrement, la CRO veillera à ce que les données d'identification des sujets de l'étude présentant une demande, telles que le nom complet, l'adresse électronique, etc. et leurs données pseudonymisées concernant la santé ne soient pas combinées dans leurs systèmes de traitement des données. Cela peut se faire en désignant des équipes différentes pour traiter les demandes des sujets de l'étude et pour traiter les données pseudonymisées relatives à la santé des sujets de l'étude collectées aux fins de la recherche primaire. Toutefois, dans les cas où la CRO reçoit une demande d'une personne concernée, elle doit s'assurer qu'elle est en mesure d'attribuer la demande à la bonne personne concernée en combinant les Identifiants et les données relatives à la santé de manière ponctuelle. Une fois l'exercice des droits terminé, la CRO supprime de ses bases de données les données directement identifiantes de la Personne concernée par l'étude, tout en conservant des documents attestant de la conformité à la demande, par exemple en expurgeant ou en hachant les identifiants directs.

Si une CRO fournit au promoteur un service direct au patient (cf liste des services à l'annexe 2, classe (8)) , les sujets de l'étude ont le droit et peuvent très probablement contacter la CRO pour lui demander d'exercer leurs droits en matière de protection des données, c'est-à-dire une demande de la part de la personne concernée, ou pour toutes autres questions. Dans ce cas, la CRO doit mettre en œuvre des dispositions spéciales en matière de sécurité, conformément à la section 3.6.3 du présent code.

4.5.5 Violations de données à caractère personnel

Conformément à l'article 4, paragraphe 12, du RGPD, on entend par "violation de données à caractère personnel" une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Il s'agit de tout incident de sécurité, malveillant ou non et survenant de manière intentionnelle ou non, ayant pour effet de compromettre l'intégrité, la confidentialité ou la disponibilité des données à caractère personnel.

La notification d'une violation de données à caractère personnel n'est pas exigée dans toutes les circonstances :

- La notification à l'autorité de contrôle compétente est exigée, sauf s'il est peu probable qu'une violation entraîne un risque pour les droits et libertés des Personnes.
- La communication d'une violation à la Personne n'est déclenchée que lorsqu'elle est susceptible d'entraîner un risque élevé pour ses droits et libertés.

Le responsable du traitement est responsable de la protection des données à caractère personnel. Cela inclut la responsabilité de chercher à contenir l'incident, d'évaluer le risque qui pourrait en résulter et de déterminer si cela est nécessaire, de notifier la violation de données à caractère personnel à l'autorité de contrôle ainsi que de communiquer la violation de données à caractère personnel à la personne concernée.

Remarque :

- Il convient de noter qu'une CRO peut effectuer une notification à l'autorité de contrôle pour le compte du responsable du traitement, si ce dernier a chargé la CRO d'effectuer des notifications en son nom et que cela fait partie des dispositions contractuelles entre la CRO et le responsable du traitement. Toutefois, il est important de noter que la responsabilité légale de la notification incombe toujours au responsable du traitement.

La CRO, quant à elle, en tant que sous-traitant des données, doit aider le responsable du traitement à assurer le respect de ses obligations.

En ce qui concerne les violations de données à caractère personnel, l'assistance fournie par la CRO consiste notamment à :

- notifier au responsable du traitement "sans retard injustifié" lorsqu'elle prend connaissance d'une violation de données à caractère personnel sans avoir au préalable évalué la probabilité du risque découlant de la violation de données à caractère personnel ; c'est le responsable du traitement qui doit procéder à cette évaluation dès qu'il prend connaissance de la violation ;
- plus généralement, en communiquant toutes les informations auxquelles la CRO a accès et qui sont nécessaires au responsable du traitement pour lui permettre de se conformer à ses obligations. Ce rapport peut être établi progressivement, au fur et à mesure que des informations plus détaillées sont disponibles ; et
- en aidant le responsable du traitement à prendre les mesures correctives appropriées pour remédier à la violation de données à caractère personnel.

Remarque :

- Lorsque la CRO fournit des services à plusieurs responsables du traitement qui sont tous affectés par le même incident, elle devra communiquer les détails de l'incident à chaque responsable du traitement.

Les modalités pratiques de l'assistance fournie par la CRO au responsable du traitement sont décrites dans le contrat relatif au traitement des données, qui doit préciser les responsabilités des parties.

4.5.5.a La CRO met en place des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adéquat des données à caractère personnel ; la capacité de détecter, de traiter et de signaler au responsable du traitement une faille de données à caractère personnel en temps utile est considérée comme un élément essentiel de ces mesures.

Par exemple, pour détecter une violation de données à caractère personnel, une CRO pourrait utiliser certaines mesures techniques telles que des analyseurs de flux de données et de journaux, à partir desquels il est possible de définir des événements et des alertes en corrélant toute donnée du journal.

4.5.5.b La CRO met en place une procédure de déclaration documentée, définissant le processus de déclaration à suivre par les employés de la CRO et tous les autres professionnels qui interviennent dans la Recherche clinique lorsqu'ils sont confrontés à un événement lié à la sécurité, afin de les aider à notifier ces informations concernant les événements liés à la sécurité à la personne responsable de la CRO (par exemple, le DPD de la CRO) ou aux personnes de la CRO chargées de traiter les incidents, afin d'établir l'existence d'une faille sécurité de données à caractère personnel.

4.5.5.c La CRO met en place une formation pour apprendre aux employés et à tous les autres professionnels qui interviennent dans la recherche clinique comment réagir face aux événements liés à la sécurité, y compris les violations de données à caractère personnel, et respecter les procédures et mécanismes mis en place par la CRO.

4.5.5.d La CRO établit un registre interne des violations de données à caractère personnel afin de documenter les violations de données à caractère personnel auxquelles elle est confrontée, qu'il s'agisse ou non d'une violation de données à caractère personnel devant être notifiée ; ce registre interne contient (i) les mêmes informations clés que celles qui doivent figurer dans le registre interne tenu par le responsable du traitement conformément à l'article 33, paragraphe 5, afin d'aider le

responsable du traitement à documenter son propre registre des violations de données à caractère personnel (ii) les enregistrements des mesures prises par la CRO pour aider le responsable du traitement à se conformer à ses obligations.

4.5.5.e La CRO dispose d'une procédure de déclaration documentée[16] à soumettre à l'accord du responsable du traitement lorsqu'elle s'engage dans une relation contractuelle, qui définit le processus à suivre pour aider le responsable du traitement en temps utile en cas de violation de données à caractère personnel, y compris, par exemple, (i) des canaux de communication efficaces (ii) des délais de déclaration (iii) une personne responsable.

4.5.5.f Lorsqu'une CRO a désigné un DPD, celui-ci doit être rapidement informé de l'existence de la violation de données à caractère personnel et impliqué tout au long du processus de gestion et de notification de la violation. Dans le cas contraire, un responsable, possédant les compétences et les connaissances nécessaires en matière de protection des données découlant d'une formation appropriée, doit être désigné pour traiter ces questions et être en contact avec le responsable du traitement.

Exemple :

- Dans le cadre d'un rapport de sécurité, un Site Investigateur envoie à la CRO des copies de dossiers médicaux d'un sujet de l'étude pour l'évaluation d'un événement indésirable. L'équipe de pharmacovigilance de la CRO a détecté que les copies des dossiers médicaux contiennent le nom complet non expurgé du sujet de l'étude, ce qui permet de réidentifier le sujet de l'étude.
  - L'employé de la CRO formé pour identifier une violation de données à caractère personnel, informe rapidement le DPD et/ou le cas échéant un autre responsable de la CRO, en utilisant le canal de communication défini dans la procédure interne de la CRO.
  - Le DPD et/ou l'autre responsable de la CRO, informe rapidement le DPD et/ou l'autre représentant du responsable du traitement en utilisant le canal de communication et les formulaires pour documenter la violation de données à caractère personnel définis dans la procédure préalablement convenue avec le responsable du traitement.
  - La CRO s'assure que cette violation de données à caractère personnel est contenue et maîtrisée. Dans le cas contraire, la CRO communique des informations documentées au fur et à mesure que des détails supplémentaires sont disponibles.
  - La CRO reste à la disposition du responsable du traitement pour l'aider à se conformer à ses obligations et demande ses instructions avant d'entreprendre toute action concernant la violation de données à caractère personnel .
  - La CRO rappelle officiellement au Site Investigateur les obligations qui lui incombent en vertu du RGPD.
  - La CRO enregistre la violation de données à caractère personnel dans son propre registre interne des violations de données à caractère personnel.

4.6 Transferts de données vers des pays tiers

Pour éviter toute ambiguïté, le Code de conduite dans sa forme actuelle n'est pas destiné à être un Code de conduite en tant qu'outil pour les transferts internationaux conformément à l'article 46, paragraphe 2, point e), du RGPD. Une CRO adhérant au Code de conduite devrait en informer le responsable du traitement et lui expliquer que l'adhésion d'une CRO au Code ne peut pas remplacer ces outils de transfert légaux.

Domaine d'application : Les exigences expliquées dans chaque section du présent chapitre s'appliquent de manière générale, c'est-à-dire à toutes les classes de services énumérées à l'annexe 2, à l'exception des classes (1) et (2).

Les transferts internationaux de données à caractère personnel entrant dans le champ d'application de la présente section comprennent les transferts de données à caractère personnel effectués dans le cadre de l'un des services couverts par le présent Code et sont soumis à l'article 44 du RGPD ;

[16] Lignes directrices sur la notification des violations de données personnelles en vertu de l'Acte réglementaire 2016/679.

"*Tout transfert de données à caractère personnel faisant l'objet d'un traitement ou destinées à être traitées après leur transfert vers un pays tiers ou vers une organisation internationale n'a lieu que si, sous réserve des autres dispositions du présent règlement, les* ***conditions prévues au" le chapitre V du RGPD "sont respectées par le responsable du traitement et le sous-traitant*** *[...]".*

4.6.a La CRO veille à ce que, pour chaque cas de transfert international de données à caractère personnel effectué dans le cadre de la fourniture de ses services, les éléments suivants soient énumérés dans le contrat au traitement des données :

1. Une description du transfert, y compris la base légale du transfert et la localisation de l'importateur, ainsi que l'évaluation de la législation applicable à l'importateur pour les transferts spécifiques lorsqu'il n'y a pas de décision d'adéquation applicable et que les transferts ne sont pas fondés sur des dérogations ;
2. Selon les instructions du promoteur, l'outil de transfert sélectionné sur la base duquel le transfert est autorisé par le RGPD, à savoir : a) décision d'adéquation en vigueur de la Commission européenne ; b) un accord fondé sur les clauses contractuelles types adoptées par la Commission européenne ; c) des règles d'entreprise contraignantes appropriées ; (d) un Code de conduite applicable au domaine de la recherche scientifique avec des engagements contraignants et exécutoires du responsable du traitement ou du sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ; (e) un mécanisme de certification approuvé conformément à l'article 42 du RGPD ; ou (f) des clauses contractuelles *ad hoc* en vertu de l'article 46, paragraphe 3, point a), du RGPD ; ou (g) l'une des dérogations prévues à l'article 49[17] , y compris le consentement des personnes concernées, lorsque des conditions spécifiques peuvent légitimer un tel transfert international ; et
3. Toute autre instruction du promoteur relative aux transferts de données à caractère personnel, y compris toute mesure supplémentaire[18] devant être adoptée, le cas échéant.

Exemple :

- Une CRO adhérant au Code mettra en œuvre les contrôles applicables à ses services conformément au document 02 et pourra proposer au promoteur d'approuver ces contrôles comme satisfaisant à l'exigence de "mesures supplémentaires" adéquates.

4.6.b La CRO fournit au promoteur des informations sur l'outil de transfert qu'il a l'intention d'utiliser, sur la base des résultats de son évaluation de l'impact des transferts ([19]) et sur les mesures de sauvegarde adoptées pour faire face à tout risque résiduel lié aux transferts internationaux.

4.6.c La CRO communique à ses sous-traitants auxquels des données sont transférées les instructions du responsable du traitement concernant le transfert de données à caractère personnel vers des Pays tiers. La CRO peut fournir des instructions supplémentaires à ses sous-traitants, à condition que ces instructions supplémentaires n'entrent pas en conflit avec les instructions du responsable du traitement des données.

17 Lignes directrices 2/2018 du CEPD sur les dérogations à l'article 49

18 Recommandations 01/2020 du CEPD sur les mesures qui complètent les outils de transfert pour garantir le respect du niveau européen de protection des données à caractère personnel, adoptées le 18 juin 2021.

19 Recommandations 01/2020 du CEPD sur les mesures qui complètent les outils de transfert pour garantir le respect du niveau européen de protection des données à caractère personnel, adoptées le 18 juin 2021.

4.6.1 La CRO en tant qu'exportateur

La présente section précise les exigences auxquelles doit satisfaire la CRO lorsqu'elle agit en tant qu'Exportateur pour le compte du responsable du traitement impliqué dans le transfert de données à caractère personnel en dehors de l'Union européenne, conformément au chapitre V du RGPD et aux recommandations du Comité européen de protection des données[20] après la décision dans l'affaire C-311/18 - Facebook Ireland et Schrems. Par conséquent, les CRO agissant en tant qu'exportateurs, le cas échéant avec l'importateur, doivent déterminer au cas par cas et en tenant compte des circonstances du transfert si la législation ou les pratiques du pays tiers de destination empêchent ou non de se conformer au niveau de protection essentiellement équivalent à celui de l'UE et, le cas échéant, compléter l'outil de transfert sélectionné par toute mesure supplémentaire appropriée. Considérant que le transfert est une activité de traitement effectuée pour le compte du promoteur (responsable du traitement), la CRO rappelle au promoteur qu'il pourrait également être tenu responsable en vertu du chapitre V du RGPD pour les transferts effectués par la CRO[21] .

Si les CRO agissant en tant qu'exportateur ne sont pas en mesure de prendre des mesures supplémentaires appropriées pour garantir un niveau de protection essentiellement équivalent en vertu du droit de l'UE, elles sont tenues de suspendre ou de mettre fin au transfert des données à caractère personnel.

Cette section couvre le scénario dans lequel il y a soit :

a. Une CRO établie dans l'UE transférant des données à caractère personnel à des sous-traitants secondaires établis dans un pays tiers (transfert dit " de sous-traitant à sous-traitant ") ; ou

b. Une CRO établie dans un pays tiers transférant des données à caractère personnel à des sous-traitants secondaires également établis dans un pays tiers lorsque le transfert concerne des données à caractère personnel de personnes concernées participant à une étude clinique et se trouvant dans l'UE (autrement appelé "transfert de sous-traitant à sous-traitant").

c. Une CRO établie dans l'UE qui transfère des données à caractère personnel à un promoteur établi dans un pays tiers (autrement dit, un transfert de " sous-traitant à responsable du traitement ") ; ou

d. Une CRO établie dans un pays tiers qui transfère des données à caractère personnel à un promoteur également établi dans un pays tiers lorsque le transfert concerne des données à caractère personnel de personnes participant à une étude clinique qui se trouvent dans l'UE (autrement appelé "transfert de sous-traitant à responsable du traitement").

Exemples :

- Une CRO internationale fournissant des services de mise en place d'étude exporte des données à caractère personnel d'investigateurs de ses entités européennes vers un sous-traitant secondaire hébergeant des données dans des pays non membres de l'UE (scénario a).
- Une CRO hébergeant un système d'EDC exporte des données à caractère personnel en répliquant les données de son centre de données de l'UE vers son centre de données de secours dans des pays non membres de l'UE (scénario a).
- Une CRO fournissant des services d'eTMF dans un pays non membre de l'UE exporte des données à caractère personnel à une autre CRO installée dans un autre pays non membre de l'UE (scénario b).
- Une CRO située dans un pays de l'UE et fournissant des services de pharmacovigilance transmet les données à caractère personnel reçues en tant qu'événements indésirables graves à l'équipe médicale d'un promoteur située dans un pays non membre de l'UE (scénario c).
- Une CRO basée dans un pays non membre de l'UE et fournissant des services de suivi médical transfère des données à caractère personnel de personnes concernées sur des Sites Investigateurs de l'UE à un Prestataire basé dans un pays non membre de l'UE (scénario d).

Il convient d'établir une distinction entre la CRO qui agit en tant qu'exportateur dans le cadre de ses propres procédures internes pour fournir ses services dans le cadre du contrat de service et une CRO qui agit en tant qu'exportateur sous la direction d'un promoteur situé en dehors de l'UE. Ce scénario peut se produire lorsque la CRO qui agit en tant qu'exportateur pour fournir ses services dans le cadre du contrat de service doit

[20] Recommandation 1/2020 du CEPDsur les mesures qui complètent les outils de transfert pour assurer la conformité avec le niveau de protection des données à caractère personnel de l'UE, et Recommandation 2/2020 du CEPD sur les garanties essentielles européennes pour les mesures de surveillance.

[21] Section 19 de la ligne directrice 5/2021 du CEPD sur l'interaction entre l'application de l'article 3 et les dispositions relatives aux transferts internationaux conformément au chapitre V du RGPD.

transférer des données à caractère personnel en raison de ses processus internes plutôt qu'à la demande du promoteur.

Exemple :

La CRO doit transférer les données du promoteur vers des pays tiers :

- à ses filiales dans les pays tiers, parce que le personnel de la CRO chargé de traiter les données dans le cadre des services est le personnel de la filiale concernée de la CRO ; ou
- À un fournisseur de services de communication informatique établi dans un pays tiers, parce que ce sous-traitant secondaire fournit à la CRO ses plateformes en ligne d'entreprise pour les vidéoconférences et les audioconférences utilisées dans les réunions des investigateurs et les visites de contrôle à distance du Site Investigateur.

La CRO doit informer le promoteur de ces transferts de données et se conformer aux exigences en matière d'autorisation conformément au paragraphe 2 de l'article 28 du RGPD.

4.6.1.a La CRO qui fournit les services au promoteur et agit en tant qu'exportateur dans le cadre de ses propres processus internes aux fins de ses services fournit au promoteur une liste des lieux de traitement de ses données, de la manière convenue avec le promoteur dans contrat sur le traitement des données, et la preuve que les dispositions du chapitre V sont respectées pour le transfert selon les instructions du responsable du traitement, y compris qu'un outil de transfert approprié est utilisé.

Exemple :

- La CRO donnera au promoteur la liste de toutes les sociétés affiliées à la CRO qui sont engagées dans le traitement du service concerné, ainsi que de tous les fournisseurs agissant en tant que sous-traitants de la CRO, le cas échéant. La CRO peut convenir avec le promoteur que la CRO donne accès à un portail web ou à un site similaire, où les informations sur les lieux de traitement sont disponibles pour le promoteur ; ou peut inclure ces listes de lieux de traitement dans le contrat sur le traitement des données.

4.6.1.b Toute CRO qui agit en tant qu'exportateur, que ce soit dans le cadre de ses propres processus internes ou sous la direction du promoteur, doit tenir des registres des transferts internationaux de données à caractère personnel qu'elle effectue pour ce promoteur, y compris la base juridique prévue au chapitre V pour chaque transfert.

Exemple :

- La CRO peut conserver les registres de transfert dans le cadre des registres des activités de traitement qu'une CRO doit tenir pour se conformer à l'article 30, paragraphe 2, du RGPD. Les registres de transfert doivent, si possible et/ou si le promoteur donne des instructions en ce sens à la CRO, indiquer, outre le pays de transfert/destination, le type ou/et le nom des sous-traitants dans le pays de destination .

4.6.2 La CRO en tant qu'importateur

Cette section précise les exigences imposées à la CRO lorsque celle-ci agit en tant qu'importateur de données à caractère personnel qui ont été transférées en dehors de l'Union européenne par un autre exportateur.

Cette section couvre le scénario dans lequel il y a soit :

e. Une CRO établie dans un pays tiers recevant des données à caractère personnel d'un promoteur établi dans l'UE (autrement appelé transfert de "responsable du traitement à sous-traitant") ; ou

f. Une CRO établie dans un pays tiers recevant des données à caractère personnel d'une autre CRO ou d'un autre sous-traitant de données établi dans l'UE (autrement appelé transfert "de sous-traitant à sous-traitant").

Exemples :

- Une CRO basée dans un pays non membre de l'UE fournissant une analyse statistique sur un ensemble de données contenant des données à caractère personnel de personnes concernées sur des sites Investigateurs de l'UE, reçues d'un promoteur basé dans l'UE (scénario e).

- Une CRO fournissant des services de pharmacovigilance hébergée aux États-Unis reçoit des données exportées par le site Investigateur pour le compte du promoteur (scénario f).

4.6.2.a La CRO qui fournit les services au promoteur et agit en tant qu'importateur aux fins de ces services, fournit au promoteur une liste des lieux de traitement des données et la preuve que les dispositions du chapitre V sont respectées pour le transfert selon les instructions du responsable du traitement, y compris qu'un outil de transfert approprié est utilisé.

4.6.2.b Toute CRO qui agit en tant qu'importateur doit fournir au responsable du traitement et à l'exportateur une assistance concernant le respect des obligations légales du responsable du traitement et de l'exportateur, y compris :

1. tenir le responsable du traitement et l'exportateur informés de toute loi ou pratique qui empêche la CRO agissant en tant que sous-traitant et importateur de maintenir un niveau de protection des données essentiellement équivalent à celui de l'UE ;
2. la mise à disposition de toutes les informations dont le responsable du traitement et l'exportateur ont besoin pour évaluer l'impact du transfert sur l'importateur ; et
3. avoir pour politique d'évaluer et de mettre en œuvre des mesures supplémentaires conformément aux instructions du responsable du traitement.

Exemple :

- La CRO indique toute loi pertinente du pays de destination dont elle a connaissance et qui peut présenter un risque pour la sécurité et la confidentialité des données à caractère personnel.

4.6.3 Transferts ou divulgations non autorisés par le droit de l'Union

Conformément à l'article 48 du RGPD, une demande d'un pays tiers de transférer ou de divulguer des données à caractère personnel ne rend pas, en tant que telle, un transfert ou une divulgation licite en vertu du RGPD. Une demande émanant d'un tribunal d'un Pays tiers ou d'une autorité ne constitue pas en soi une base juridique pour un tel transfert ou une telle divulgation. Un jugement d'une juridiction et toute décision d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un Sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peuvent être reconnus ou exécutoires que s'ils sont fondés sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du chapitre V du RGPD.

En l'absence d'un cadre fourni par un accord international ou par une autre base juridique en vertu du RGPD assortie d'un motif de transfert, conformément au chapitre V du RGPD, les ORC soumis au droit de l'UE ne peuvent légalement fonder la divulgation et le transfert de données à caractère personnel sur ce type de demande.

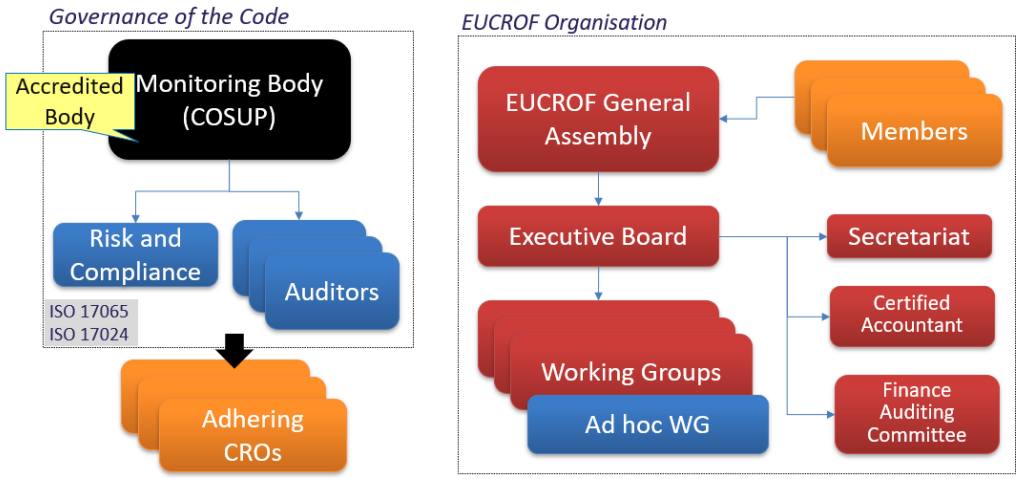
5 Contrôle et Conformité

5.1 Gouvernance du code

Avec ce Code, EUCROF désigne un organe interne, appelé Comité de surveillance (ci-après également dénommé COSUP), doté de toutes les capacités requises conformément à l'article 41 du RGPD "*Surveillance des codes de conduite approuvés*".

Le COSUP est l'organisme qui possède "*le niveau d'expertise approprié par rapport à l'objet du code et qui est accrédité par l'autorité de contrôle compétente*", tel que défini à la section 1.4 (5) du présent code.

Le COSUP est le seul organe habilité à prendre des décisions opérationnelles concernant le respect du code par les CRO.



Le schéma ci-dessus décrit l'organisation de la gouvernance du Code en tant que structure interne (cadre de gauche), indépendante des organes décisionnels et exécutifs de l'EUCROF (cadre de droite).

Le COSUP est l'organisme accrédité par l'Autorité de contrôle compétente conformément au processus officiellement établi avant l'entrée en vigueur du Code de conduite. Le COSUP délègue certaines de ses tâches au responsable des risques et de la conformité, qui effectue également des audits internes réguliers et recrute des auditeurs chargés de contrôler les candidats ayant choisi de chercher à obtenir une marque de conformité au code EUCROF de niveau 2, sur la base d'audits sur place. Le groupe de travail *ad hoc* est un groupe de travail temporaire dont la Finalité est d'identifier et de proposer des candidats pour le COSUP et de documenter ces candidatures.

5.1.1 Indépendance et impartialité

Pour garantir l'indépendance, l'impartialité et l'absence de conflits d'intérêts, les processus régissant les activités du COSUP doivent être conformes aux normes ISO 17065 "*Exigences pour les organismes certifiant des produits, des processus et des services*" et 17024 "*Évaluation de la conformité - Exigences générales pour les organismes procédant à la certification de personnes*".

En ce qui concerne l'impartialité, elle est assurée par :

- La politique d'impartialité et de lutte contre la corruption du COSUP ;
- les procédures relatives à l'audit et à l'audit à distance, qui précisent, entre autres, la manière de sélectionner et d'interroger les auditeurs, afin d'éviter les conflits d'intérêts et, respectivement, les risques de corruption ; et
- la procédure relative à la prise de décision par le COSUP, qui spécifie, entre autres, la manière d'éviter une éventuelle influence des membres et des auditeurs.

Les opérations et les coûts fixes du COSUP doivent être couverts par les frais d'audit et d'évaluation facturés aux adhérents. Toutefois, l'EUCROF, en tant que porteur du code, s'engage à garantir au COSUP les moyens de son bon fonctionnement en lui attribuant une subvention (approuvée par l'assemblée générale d'EUCROF sur la base d'un budget prévisionnel annuel) de façon à compléter, s'il y a lieu, les revenus issus des adhésions payées par les adhérents au code.

Le budget du COSUP sera géré par son président, sans interférence ou instruction de la part du porteur du code et le COSUP aura le contrôle de ses propres comptes bancaires et de ses paiements.

La procédure relative aux ressources humaines et le manuel de gouvernance et de qualité garantissent que le COSUP dispose d'un personnel et d'une direction, d'une responsabilité et d'une fonction distincts de ceux de l'EUCROF et qu'elle évalue les performances de ses auditeurs. Les procédures d'audit et de prise de décision susmentionnées garantissent qu'il existe des barrières organisationnelles et informationnelles et des structures de gestion distinctes pour le porteur du code et du COSUP, et que cet dernier agit sans recevoir d'instructions de l'EUCROF.

5.1.2 Responsabilité juridique

Le COSUP a le statut approprié pour exercer son rôle en vertu de l'article 41, paragraphe 4, du RGPD et est l'organe responsable en dernier ressort de la prise de décision conformément à la section 5 du présent Code. Néanmoins, en tant qu'organe interne, le COSUP ne dispose pas d'une capacité juridique autonome pour être tenu responsable de l'exécution de ses tâches et de ses fonctions, en vertu de l'article 83, paragraphe 4, du RGPD. À ce titre, conformément à l'article 83, paragraphe 4, point c), du RGPD "*Conditions générales pour l'imposition d'amendes administratives*" et compte tenu du fait que (a) l'EUCROF est le porteur du présent Code et, (b) que le COSUP est un organe interne, l'EUCROF en tant qu'entité juridique responsable au titre de la surveillance du présent Code de conduite et du processus d'adhésion, assumera l'entière responsabilité de tout manquement aux obligations du COSUP en vertu de l'article 41, paragraphe 4, du RGPD, et dispose de toutes les assurances et réserves nécessaires pour couvrir les risques inhérents à cette responsabilité.

Quoi qu'il en soit, l'organisme de contrôle (COSUP) est responsable, devant l'autorité de contrôle, de toutes ses actions et décisions liées à ses activités, et le porteur du code doit prendre les mesures nécessaires pour que cette responsabilité puisse être pleinement exercée.

5.2 Le comité de surveillance (COSUP)

5.2.1 Composition

Le COSUP est composé d'un maximum de 12 membres, à moins qu'un nombre plus élevé ne soit décidé par l'Assemblée Générale de l'EUCROF.

Les membres sont des personnes physiques ayant un minimum de 10 ans d'expérience dans au moins un des domaines suivants : (1) la recherche dans les domaines de la santé, de l'épidémiologie, de la génétique, des biostatistiques, des sciences humaines et sociales, (2) la protection des données à caractère personnel, (3) les systèmes d'information sur la santé, (4) la protection des droits des patients, ou (5) une expérience pertinente des processus d'audit, d'inspection ou de certification.

La composition du COSUP doit garantir que tous ces principaux domaines d'expertise seront représentés au sein du COSUP et que, par conséquent, le COSUP comptera obligatoirement des représentants ayant l'expérience requise en matière de protection des données. En outre, tous les membres du COSUP auront l'exigence d'avoir suivi une formation sur la Protection des données à caractère personnel et sur le Code lui-même.

La composition du COSUP doit refléter une représentation équilibrée des parties prenantes intéressées par le code et doit répartir équitablement le nombre de membres de chaque catégorie, et cette répartition équilibrée doit être maintenue dans le cas où la taille du COSUP est augmentée par décision de l'Assemblée Générale de l'EUCROF. Ainsi, les membres du COSUP comprennent un minimum de deux (2) et un maximum de trois (3) représentants de chaque catégorie ci-dessous :

- CROs ;
- Associations ou défenseurs des patients,
- Professionnels de santé (sites Investigateurs),

- Les organisations qui produisent ou commercialisent des produits de santé, y compris les sociétés pharmaceutiques, les fabricants de dispositifs médicaux et les sociétés de biotechnologie ; et
- Experts indépendants possédant une expérience documentée dans un ou plusieurs des domaines susmentionnés[22] .

Les membres doivent tous être employés par des entreprises/organisations différentes, ce qui signifie que deux (2) membres du COSUP ne peuvent pas être employés par la même entreprise/organisation. Dans tous les cas, les membres ne peuvent pas également siéger dans l'un des autres organes décisionnels de l'EUCROF : le Bureau exécutif, le Bureau des membres titulaires ou l'Assemblée générale.

5.2.2 Président et Vice-président

Le Président et le Vice-Président du COSUP sont élus par et parmi les membres du COSUP. Lors d'une mandature, une seule de ces fonctions peut être occupée par un membre ayant également des fonctions dans une CROs. Sous réserve de la procédure d'initiation décrite à la section 5.2.6, ils sont élus par un vote à la majorité simple de tous les membres du COSUP.

5.2.3 Conditions d'adhésion

La durée du mandat des membres du COSUP est de 3 ans. Un membre régulier peut voir la durée de son mandat prolongée pour 3 mandats successifs de 3 ans.

La durée du mandat du Président et du Vice-Président est également de 3 ans et ne peut être prolongée qu'une seule fois après réélection, ce qui signifie que la durée maximale pendant laquelle un Membre peut remplir le rôle de Président ou de Vice-Président du COSUP est de 6 ans. Le Président ou le Vice-Président du COSUP, ayant terminé son mandat de 6 ans, peut cependant continuer en tant que membre ordinaire conformément aux règles applicables aux membres ordinaires ou demander à assumer le rôle qu'il n'avait pas auparavant.

5.2.4 Pouvoirs

Le COSUP remplit les fonctions suivantes :

a) Examine et évalue les demandes et les dossiers de conformité soumis par les CROs désireuses d'adhérer au Code et décide de la marque de conformité au Code de l'EUCROF appropriée pour les candidats retenus.

b) Fournit des instructions appropriées pour la mise à jour du registre public en ligne des CROs adhérentes.

c) Prend des décisions concernant la sélection des auditeurs et enregistre les auditeurs approuvés dans le panel des auditeurs.

d) Organise et approuve l'affectation des auditeurs chargés d'évaluer les CROs qui ont demandé à adhérer au Code dans le cadre du programme d'audit visé au point 5.5.6.

[22] Un exemple de composition reflétant une représentation équilibrée des membres pourrait être le suivant : 11 membres du COSUP comprenant

- 1 Délégué à la Protection des données à caractère personnel d'une CRO, 1 délégué à la qualité d'une CRO, ainsi que 2 représentants des CROs.
- 1 responsable opérationnel d'une association de patients, 1 conseiller juridique qui défend les droits des patients, ainsi que 2 représentants d'associations de patients ou de défenseurs des droits des patients.
- 1 membre d'un Comité Central d'Éthique national, 1 chercheur principal d'un hôpital universitaire agissant en tant que Site Investigateur, ainsi que 2 représentants des Professionnels de la Santé (Sites Investigateurs).
- 1 responsable de la protection de la vie privée d'une entreprise pharmaceutique, 1 Responsable de la Sécurité de l'Information d'une entreprise de technologie médicale, ainsi que 2 représentants d'organisations produisant ou commercialisant des produits de santé, y compris des entreprises pharmaceutiques, des fabricants de dispositifs médicaux et des entreprises de biotechnologie.
- 1 consultant indépendant en audit de sécurité, 1 consultant indépendant expert en essais décentralisés et 1 directeur d'une organisation de biobanques, soit 3 représentants qui sont des experts indépendants ayant une expérience documentée dans un ou plusieurs des domaines susmentionnés.

e) Prend des décisions concernant la sélection du Responsable interne des Risques et de la Conformité dont le rôle est précisé au point 5.4 ci-après.

f) Élabore et propose à l'Assemblée Générale de l'EUCROF, pour décision de vote, les marques de conformité au Code de l'EUCROF qui peuvent être utilisées par les CROs adhérentes.

g) Organise et contrôle le maintien de la conformité des CROs adhérentes à intervalles réguliers, comme défini dans les procédures du Code concernant le processus de contrôle et de maintien de la conformité au Code.

h) Établit des procédures et des structures pour traiter les plaintes concernant des infractions au Code ou la manière dont le Code a été, ou est, mis en œuvre par les CROs. Conformément à la section 74 des *lignes directrices 1/2019 du* CEPD *sur les Codes de Conduite et les organismes de contrôle en vertu de l'Acte réglementaire 2016/679*, ces procédures seront mises à la disposition du public sur le site internet de l'EUCROF.

i) Missionne et contrôle les plaintes concernant les infractions au Code commises par les CROs adhérentes.

j) Prend les mesures appropriées à l'encontre d'une CRO en cas d'infraction au Code ou dans le cas où une CRO ne fournit pas au COSUP les informations nécessaires à l'investigation d'une éventuelle infraction au Code.

k) Conformément à l'article 41, paragraphe 4, du RGPD, informe l'autorité de contrôle compétente des mesures finales prises à l'encontre des CRO et des raisons qui les ont motivées. En cas de suspension ou d'exclusion de la CRO, l'autorité de contrôle compétente est informée sans délai.

l) Met en œuvre des procédures et des structures qui préviennent les conflits d'intérêts.

m) Communique avec le grand public, selon les exigences, afin d'assurer une transparence appropriée. À cette fin, le COSUP a la capacité de donner des instructions appropriées pour la mise à jour du site internet de l'EUCROF et les organes correspondants de l'EUCROF mettent en œuvre ces instructions avec une diligence raisonnable.

n) Assurer une gestion financière appropriée et fournir des rapports d'information à l'Assemblée Générale de l'EUCROF[23] ;

o) Élabore et met en œuvre toutes les procédures pertinentes pour s'assurer que les opérations du COSUP sont conformes aux normes ISO 17065 et 17024 et sont correctement documentées, organise des audits internes si nécessaire et, à cette fin, coordonne le cas échéant avec le Responsable des Risques et de la Conformité, afin d'obtenir et de conserver son accréditation par l'autorité de contrôle compétente.

p) Suit les changements dans les lois de l'Union européenne sur la protection des données et d'autres lois pertinentes et propose des changements pertinents au Code dans les trois mois suivant des changements importants dans ces lois sur la protection des données. À cette fin, le COSUP a la capacité d'activer les groupes de travail pertinents de l'EUCROF ou de mettre en place des groupes de travail *ad hoc* si nécessaire.

q) Contribue à l'amélioration continue du code en analysant les pratiques quotidiennes (rapports d'audit, traitement des plaintes, etc.) et en élaborant des recommandations d'amélioration à l'intention du porteur du Code (EUCROF).

r) Examine les mises à jour du Code, avant qu'elles ne soient soumises à l'Autorité de contrôle compétente par le porteur du Code (EUCROF).

Il convient de noter que l'introduction de modifications au Code relève de la responsabilité du porteur du Code (EUCROF). Le porteur du Code informe l'autorité de contrôle compétente des modifications envisagées avant leur entrée en vigueur et, si l'autorité de contrôle compétente le juge nécessaire, une nouvelle approbation du Code peut être requise avant l'entrée en vigueur de ces modifications.

[23] L'Assemblée Générale n'exerce aucun contrôle sur la gestion financière du COSUP, de sorte que ce rapport n'a qu'une valeur informative.

5.2.5 Conflits d'intérêts, impartialité et indépendance

Au moment de leur nomination, les membres du COSUP remplissent une déclaration d'intérêts directs ou indirects avec des organisations qui ont adhéré ou pourraient adhérer au Code, ainsi qu'avec les clients de ces organisations.

En outre, une procédure de déclaration des conflits d'intérêts potentiels sera mise en œuvre avant chaque réunion du COSUP en tant que point permanent de l'ordre du jour de la réunion. Cette procédure exclut du vote les membres ayant un conflit d'intérêts potentiel (par exemple, avec une CRO qui demande à adhérer au Code).

Si le Président est en conflit d'intérêts, le Vice-Président préside la partie concernée de l'ordre du jour de la réunion et le vote associé. Si le Vice-Président est également en situation de conflit d'intérêts, la partie concernée de l'ordre du jour de la réunion et le vote y afférent sont présidés par tout autre membre qui n'est pas en situation de conflit d'intérêts.

Le modèle de déclaration d'intérêt direct ou indirect est annexé au présent Code à l'annexe 4.

Conformément à la section 68 des *lignes directrices 1/2019 du* CEPD *sur les Codes de Conduite et les organes de surveillance en vertu du règlement 2016/679,* le COSUP :

- Doit rester libre de toute influence extérieure, directe ou indirecte, et ne doit ni solliciter ni accepter d'instructions d'une personne, d'une organisation ou d'une association quelconque.
- Le COSUP dispose de son propre personnel, choisi par lui ou par un autre organisme indépendant du porteur du Code, et le personnel du COSUP est soumis à la direction exclusive du COSUP.
- Le COSUP est protégé contre toute forme de sanction ou d'ingérence (directe ou indirecte) de la part du porteur du Code, d'autres organismes compétents ou des membres du COSUP dans le cadre de l'accomplissement de ses tâches.

Les membres du COSUP sont tenus de signer un engagement d'indépendance et de confidentialité. Le modèle d'engagement d'indépendance et de confidentialité est annexé au présent Code à l'annexe 5 et fait partie intégrante du Code.

L'impartialité et l'absence de conflits d'intérêts des membres du COSUP sont gérées conformément aux exigences de la norme ISO 17065.

5.2.6 Installation du COSUP

Le recrutement des candidats au COSUP est effectué par un groupe de travail *ad hoc* formé par l'Assemblée Générale de l'EUCROF.

La création de ce groupe de travail *ad hoc* et son fonctionnement suivent les règles standard applicables à tous les groupes de travail de l'EUCROF :

- Sur approbation du conseil des membres titulaires ou de l'Assemblée Générale de l'EUCROF, le Bureau exécutif de l'EUCROF lance un appel à volontaires à tous ses membres.
- Les volontaires ne recevront aucune compensation financière pour le temps consacré à leur participation aux activités du groupe de travail *ad hoc.*
- Les frais de voyage et d'hébergement reçus sont couverts par le budget de l'EUCROF conformément à la politique financière et à la gestion de l'EUCROF.
- Le Président du groupe de travail *ad hoc* est élu par les participants lors de sa première réunion.
- Compte tenu de la tâche qui lui a été confiée, ce groupe de travail, une fois mis en place, a toute latitude pour inviter des représentants de toutes les parties prenantes intéressées par le Code à participer à ses activités.

Les tâches assignées à ce groupe de travail sont les suivantes :

- Identifier et contacter les candidats potentiels ;
- Documenter l'éligibilité des candidats ;

- Veiller à ce que la composition du COSUP proposée soit conforme aux exigences de la section 5.2.1 ci-dessus ;
- Présenter les membres proposés à l'Assemblée Générale de l'EUCROF qui approuvera formellement chacun des candidats par un vote ; et
- Une fois la composition approuvée, demander aux membres de présenter des candidats aux postes de Président et de Vice-Président, fixer la date de la première réunion du COSUP et distribuer l'ordre du jour, qui sera consacré au vote sur les postes de Président et de Vice-Président.

Les candidats aux postes de Président et Vice-Président doivent être prêts à présenter leur candidature et leurs projets au COSUP lors de la première réunion du COSUP nouvellement installé. Le COSUP vote sur le poste de Président et de Vice-Président lors de la première réunion du COSUP, après quoi les candidats retenus sont immédiatement installés et le groupe de travail est ensuite dissous afin que le COSUP puisse accomplir ses tâches et exercer ses pouvoirs de manière indépendante.

5.2.7 Prise de décision

Chaque membre du COSUP dispose d'une voix. Les voix prépondérantes peuvent être exprimées par écrit à condition qu'elles le soient avant la date limite spécifiée à chaque fois. Lorsque le vote est appelé à avoir lieu lors d'une réunion du COSUP, les voix prépondérantes peuvent être exprimées par écrit jusqu'à l'heure d'ouverture de la réunion.

Les décisions du COSUP sont prises à la majorité simple de ses membres, à condition que le quorum soit atteint.

L'avis du Président sur le contenu d'une résolution n'est pas décisif. Les membres peuvent présenter des amendements à une résolution au moment du vote sur cette résolution.

Si le quorum n'est pas atteint, les représentants présents décident, à la majorité simple des représentants présents, soit de reporter le vote à la prochaine réunion, soit de lancer un appel à voter par écrit dans un délai de 15 jours calendaires.

Toutes les résolutions approuvées par le COSUP sont inscrites dans un registre spécifique.

5.2.8 Réunions, quorum et méthodes de travail

Le COSUP se réunit de manière régulière et programmée au moins une fois tous les deux mois, soit en personne, soit par voie électronique, par exemple par téléconférence. Le Président peut également, de sa propre initiative ou à la demande d'un membre ou du Responsable des Risques et de la Conformité, convoquer une réunion du COSUP à tout moment, selon les exigences de l'exercice de ses activités.

Le COSUP ne peut atteindre le quorum que si le Président ou le Vice-Président et la moitié des autres membres au moins assistent à la réunion. Si le quorum n'est pas atteint, la réunion est ajournée et reportée jusqu'à ce que le quorum soit atteint.

Les réunions du COSUP ne sont pas publiques, mais le COSUP peut demander à des experts externes de fournir des informations sur des sujets pertinents ou d'assister à la réunion en tant qu'invités sans droit de vote.

L'ordre du jour est envoyé par courrier électronique par le Président ou le Vice-Président à tous les invités, au moins une semaine calendaire avant la réunion, en précisant les points particuliers nécessitant un vote des membres du COSUP.

Les questions traitées lors de chaque réunion du COSUP font l'objet d'un Procès-Verbal établi par l'un des membres désigné par le Président au début de la réunion. Ce Procès-Verbal est distribué à tous les membres du COSUP et, le cas échéant, révisé. Ce Procès-Verbal est voté pour approbation au plus tard lors de la réunion suivante du COSUP.

Le COSUP peut définir d'autres règlements ou mandats dans lesquels il précise ses méthodes de travail.

5.3 Le Responsable des Risques et de la Conformité

Le COSUP organise le recrutement du Responsable des Risques et de la Conformité conformément à ses procédures en matière de ressources humaines. En particulier, le COSUP s'assure que le Responsable des Risques et de la Conformité possède l'expérience, les qualifications, l'intégrité professionnelle, l'indépendance et l'impartialité requises (notamment en veillant à l'absence de conflit d'intérêts) pour remplir ses fonctions.

Le Responsable des Risques et de la Conformité est chargé de :

- l'élaboration et la mise en œuvre des processus, procédures, enregistrements et modèles nécessaires à l'accréditation du COSUP en tant qu'organisme de contrôle du Code, conformément aux exigences des normes ISO 17065 et ISO 17024, dans le cadre des exigences du Code ;
- l'élaboration des processus, des procédures et de la documentation d'appui permettant d'évaluer le respect des exigences du Code par les CROs ;
- l'élaboration du matériel pédagogique pour la formation des auditeurs, afin d'évaluer leur respect des exigences du Code, la formation et la qualification des auditeurs et le contrôle périodique de leurs performances au cours des périodes d'adhésion, afin de garantir le maintien de la conformité au Code ;
- la rédaction de la déclaration anti-corruption qui doit être signée par les membres du COSUP, les auditeurs, le Responsable des Risques et de la Conformité et toute autre personne travaillant pour le compte de l'organe de surveillance ;
- l'examen des rapports d'audit et, éventuellement, leur amélioration ;
- la communication au COSUP des recommandations des auditeurs en ce qui concerne l'évaluation d'une CRO suivant le schéma d'audit dans le cadre du processus de la marque de conformité au Code de l'EUCROF de niveau 2 ; et
- la fourniture de conseils au COSUP, chaque fois que cela est demandé.

Tous les rapports d'audit sont rédigés en anglais, afin de permettre l'examen du rapport par le Responsable des Risques et de la Conformité à l'aide du modèle du COSUP, de manière à obtenir un rapport uniforme, quel que soit le pays de l'entité auditée. Les rapports peuvent également être traduits dans les langues nationales ou régionales (dans le cas de la Belgique, de la Suisse et de l'Espagne) en usage.

Le Responsable des Risques et de la Conformité élabore le programme de formation des auditeurs en collaboration avec le COSUP. Le COSUP approuve le programme de formation avant sa première mise en œuvre. Le programme de formation est susceptible d'être modifié en fonction des lacunes observées dans la mise en œuvre du processus d'audit ou dans les rapports d'audit.

Une supervision inattendue des auditeurs peut avoir lieu au cours de leurs contrôles afin d'évaluer la manière dont ils effectuent leurs contrôles et de s'assurer de leur amélioration continue et de leur efficacité.

Le Responsable des Risques et de la Conformité doit avoir une expérience considérable en matière d'audit, avec plus de 40 audits réalisés sur la base d'une norme ISO reconnue, ainsi qu'une solide expérience en matière de conformité et de risque, d'évaluation des rapports d'audit et de qualification et de formation d'autres auditeurs.

5.4 Les auditeurs

Dans certaines circonstances décrites au point 5.5 du présent Code, l'évaluation du respect des exigences du Code par une CRO éligible peut être effectuée au moyen d'audits sur place (dans les locaux de la CRO).

À cette fin, le COSUP mettra en place une équipe d'"auditeurs" (ci-après également dénommée "panel d'auditeurs") chargée d'effectuer des audits des CROs candidates selon les modalités définies par le COSUP et le Responsable des Risques et de la Conformité.

La décision d'inscrire un candidat auditeur dans le panel des auditeurs relève de la responsabilité exclusive du COSUP, est documentée et fait l'objet d'un vote formel de ce même COSUP.

5.4.1 Qualification des auditeurs

Les auditeurs doivent avoir une expérience documentée de l'audit des normes ISO 9001 ou ISO 27001, une bonne connaissance d'autres normes applicables internationalement reconnues telles que la norme ISO 27701 ou la norme NIST SP 800-53, une compréhension approfondie des questions de protection des données, une excellente connaissance des exigences du présent Code et une connaissance suffisante des activités des CROs.

Ils doivent être déjà accrédités en tant qu'auditeurs et justifier d'une expérience de plus de 15 audits dans le même domaine ou dans un domaine connexe, y compris des audits ou une expérience professionnelle connexe dans des organisations dont les activités sont similaires à celles des CROs.

Avant d'être affectés à leur première mission d'audit conformément à la section 5.4.2, les auditeurs suivront une formation de trois jours avec un programme qui couvre les normes ISO 9001, ISO 27001, ISO 17024, ISO 17021-1, le RGPD et le présent Code par le Responsable des Risques et de la Conformité et un ou plusieurs membres du COSUP, conformément à la procédure des ressources humaines du COSUP.

5.4.2 Affectation d'un auditeur à une mission d'audit

Lorsqu'une CRO doit faire l'objet d'un audit de conformité au Code en vertu de l'article 5.5, il est de la responsabilité et de la décision exclusives du COSUP d'affecter un auditeur à cette mission d'audit.

Conformément à ses procédures opérationnelles approuvées, le COSUP identifie un auditeur du panel d'auditeurs, sous réserve que cet auditeur n'ait aucun conflit d'intérêts en rapport avec la mission d'audit qui lui a été confiée. L'auditeur est alors invité à signer une "déclaration d'absence de conflit d'intérêts" conformément aux instructions du COSUP.

Dès réception de cette déclaration, le COSUP est habilité à charger formellement l'auditeur d'effectuer, en son nom, la mission d'audit. Cette instruction prend la forme d'un document écrit et repose sur une résolution formelle (par un vote) du COSUP.

5.4.3 Conditions générales des audits

Un auditeur affecté à une mission d'audit a accès au dossier de documentation préparatoire recueilli auprès de la CRO concernée pour établir son plan d'audit.

Le dossier de documentation préparatoire contient (a) la déclaration d'applicabilité de la CRO candidate et (b) pour chaque exigence applicable, la réponse de la CRO sur la manière dont il se conforme à cette exigence. Le cas échéant, cette réponse peut nécessiter de joindre des documents supplémentaires tels que des procédures opératoires standard (POS), des politiques ou des enregistrements spécifiques.

L'auditeur prend contact avec la CRO concernée dans les deux semaines suivant la date de l'affectation et dispose d'un délai maximum de cinq semaines pour convenir d'une date d'audit.

L'auditeur envoie sa proposition de plan d'audit à la personne responsable de la CRO au moins trois semaines avant la date de l'audit et la CRO a la possibilité de poser des questions et de faire des suggestions pour modifier le plan d'audit.

Le nombre d'auditeurs et la durée d'un audit dépendent de la taille, des activités et de la complexité de la CRO à contrôler, et peuvent généralement durer d’un à trois jours.

L'audit commence par une réunion d'ouverture au cours de laquelle les auditeurs se présentent, ainsi que les objectifs et les modalités de l'audit, et rappellent à la CRO auditée comment soumettre des appels ou des plaintes conformément à la section 5.7.1 du Code. La personne responsable de la CRO présente ensuite les personnes concernées de la CRO et donne aux auditeurs des informations générales sur la gestion des locaux, par exemple la réglementation en matière d'incendie et les règles de santé et de sécurité des locaux.

L’audit ne devrait pas concerner les dossiers médicaux individuels contenant des Données de santé/ Données médicales personnelles identifiables, mais dans tous les cas, les auditeurs sont soumis au secret professionnel et ne sont pas autorisés à retirer les données de santé de leur lieu de stockage pour les inclure dans les rapports d'audit.

À la fin de l'audit, les auditeurs disposent de suffisamment de temps (comme convenu dans le calendrier d'audit) pour préparer seuls un projet de rapport contenant la liste des non-conformités identifiées, des domaines à améliorer et des points forts.

L'auditeur invite ensuite les représentants de la CRO à assister à une réunion de clôture à la fin de l'audit, au cours de laquelle il présente les principales conclusions de l'audit, y compris les non-conformités répertoriées, les domaines d'amélioration et les points forts de la CRO, ainsi que les explications et/ou les preuves appropriées de ses remarques.

L'auditeur doit communiquer les constatations de l'audit à la CRO par écrit, à l'intention de cette dernière. En fonction des résultats de l'audit, la CRO envoie dans les cinq jours ouvrables un plan d'action correctif pour acceptation par le vérificateur.

5.4.4 Présentation des rapports d'audit

Après avoir reçu et accepté le plan d'action corrective de la CRO, l'auditeur dispose de 5 jours ouvrables pour finaliser le rapport d'audit, y compris sa recommandation d'approbation de l'adhésion, d'approbation conditionnelle en cas de non-conformités mineures auxquelles la CRO remédiera en mettant en œuvre le plan d'action corrective, ou de rejet en cas de non-conformités majeures auxquelles le plan d'action corrective ne permet pas de remédier. En cas de non-conformité, l'auditeur joint également à son rapport le plan d'action correctif convenu avec la CRO.

Le rapport d'audit est signé par l'auditeur et transmis (a) à la CRO candidate et (b) au Responsable des Risques et de la Conformité pour examen. Des moyens électroniques appropriés sont utilisés pour cette transmission et comprennent un horodatage et une piste d'audit appropriés.

La CRO candidate et le Responsable des Risques et de la Conformité disposent d'une semaine à compter de la réception du rapport d'audit pour faire part de leurs remarques respectives, après quoi l'auditeur finalise le rapport d'audit.

L'ensemble du rapport final est ensuite soumis par le Responsable des Risques et de la Conformité au COSUP pour décision.

5.4.5 Frais d'audit

Les auditeurs sont payés par le COSUP, sur la base du devis approuvé et des factures correspondantes fournies par l'auditeur. Les paiements sont effectués selon les conditions définies dans la politique financière du COSUP.

Les dépenses éligibles comprennent les honoraires journaliers convenus dans le devis et les frais de voyage et d'hébergement sur la base des reçus. Ce montant total, y compris les frais de gestion facturés par le COSUP, est ensuite imputé à la CRO auditée par le COSUP.

5.5 Conditions d'adhésion

5.5.1 Éligibilité

Toute CRO telle que définie à la section 1.2 et dont les activités sont énumérées à l'annexe 1 du présent Code (section 1.7) est éligible et peut adhérer au Code. Ceci s'applique aussi bien aux membres de l'EUCROF qu'aux non-membres.

Une CRO qui s'engage dans la procédure d'adhésion est ci-après dénommée "CRO candidate".

5.5.2 Approbation de l'adhésion

La décision d'approuver une CRO candidate comme adhérant au Code relève de la responsabilité exclusive de l'organe de surveillance (COSUP) et fait l'objet d'une décision formelle par le biais d'un vote des membres du COSUP sous réserve de la section 5.2.7 du présent Code.

Cette décision n'est prise qu'après examen d'un dossier de documentation soumis par la CRO et le paiement d'une taxe de candidature. Ce dossier est d'abord examiné par le Responsable des Risques et de la Conformité, qui en vérifie (a) l'admissibilité et (b) l'exhaustivité. Le Responsable des Risques et de la

Conformité ajoute son rapport d'examen au dossier de documentation sur l'adhésion avant de le soumettre au COSUP. Lorsque la CRO a choisi de demander une marque de conformité au Code de l'EUCROF de niveau 2, le COSUP reçoit également le rapport d'audit final du Responsable des Risques et de la Conformité.

La décision du COSUP est horodatée et documentée, les arguments de justification expliqués dans un rapport écrit signé par le président du COSUP et adressé à la CRO candidate.

Les CRO candidates dont l'adhésion a été approuvée mais qui ne sont pas membres de l'EUCROF devront s'acquitter de la cotisation annuelle publiée sur le site internet de l'EUCROF avant que leur adhésion ne soit confirmée dans le registre public. Ces CROs n'auront pas droit à leur marque de conformité au Code de Conduite de l'EUCROF avant que la cotisation ne soit payée.

5.5.3 Registre public

Un registre des CROs adhérentes est mis à la disposition du public pour consultation en ligne sur le site internet de l''EUCROF. Ce registre est ci-après dénommé "registre public" et constitue la seule liste officielle des CROs adhérentes.

Il est de la responsabilité exclusive du COSUP de maintenir et de mettre à jour ce registre public de manière appropriée. Les changements dans le statut d'adhésion d'une CRO donnée sont reflétés dans le registre public sans délai excessif et au plus tard cinq (5) jours ouvrables après que le changement s'est produit. Ce délai est publié sur le site internet de l'EUCROF et dans le registre public.

Chaque enregistrement du registre public est horodaté et contient toutes les informations essentielles concernant l'adhésion de chaque CRO répertoriée. Des exemples d'informations essentielles sont : la marque de conformité au Code de l'EUCROF (déclarative ou basée sur l'audit), la date d'approbation et la référence à la décision du COSUP correspondante, la date du prochain renouvellement, etc...

5.5.4 Niveaux d'adhésion

Le Code prévoit différents niveaux de validation de l'adhésion pour les CROs candidates. Les différents niveaux de validation de l'adhésion ne reflètent que les niveaux et les méthodes de preuve qui sont soumis au COSUP. Les CROs adhérentes doivent se conformer à toutes les dispositions du Code, quel que soit le niveau de reconnaissance d'adhésion pour lequel la CRO candidate postule.

Le niveau est le choix exclusif de la CRO candidate et ce choix doit être fait avant d'engager la procédure d'adhésion car il déterminera la procédure applicable Dans les deux cas, c'est au COSUP qu'il incombe en dernier ressort de décider d'accorder ou non l'adhésion à la CRO.

5.5.5 Niveau 1 : une procédure d'adhésion déclarative

Dans la procédure d'auto-attestation ou d'adhésion déclarative " (ou " procédure de niveau 1 "), c'est la CRO candidate qui remplit et génère seule le dossier d'adhésion et le COSUP n'intervient qu'au moment où la CRO soumet son dossier d'adhésion.

Dans le cadre de cette procédure de niveau 1, la CRO candidate doit remplir un "profil d'organisation" et fournir une documentation détaillée prouvant la conformité à toutes les exigences applicables conformément à leur déclaration d'applicabilité. La documentation est accompagnée d'une liste de pièces justificatives soumises dans un format appelé « questionnaire de conformité »

Les modèles de "profil d'organisation" et de "questionnaire de conformité" sont des documents validés par le COSUP et sont accessibles sur le site internet de l'EUCROF. Le "questionnaire de conformité" est aligné sur les exigences énumérées dans le Code.

En plus de ce qui précède, la CRO candidate doit signer une "Déclaration d'exactitude et d'exhaustivité" des informations contenues dans le dossier de documentation sur l'adhésion et soumettre le dossier de documentation sur l'adhésion par le biais du site internet de l'EUCROF.

Les documents relatifs à l'adhésion sont examinés par le Responsable des Risques et de la Conformité, qui en vérifie (a) l'admissibilité et (b) l'exhaustivité, et le transmet au COSUP, accompagné du rapport d'examen du Responsable des Risques et de la Conformité.

Le COSUP analyse l'éligibilité de la CRO candidate en examinant le dossier de documentation d'adhésion soumis avec le rapport d'examen du Responsable des Risques et de la Conformité. Les membres du COSUP

déterminent si chaque exigence du Code applicable selon la déclaration d'applicabilité de la CRO a été suffisamment prise en compte dans cette documentation et si la documentation fournie permet au COSUP de contrôler la conformité de la CRO. Le COSUP a le pouvoir d'exiger de la CRO candidate qu'elle fournisse des preuves supplémentaires de conformité, par exemple plus de documentation. Le dossier de documentation sur l'adhésion sera traité par le COSUP dans un délai maximum qui sera publié sur le site internet de l''EUCROF, et une décision sera communiquée à la CRO candidate conformément à la section 5.5.2.

Le COSUP conservera la responsabilité de décider, en dernier ressort, de valider ou non l'adhésion de la CRO candidate.

À tout moment au cours de la période de trois ans pendant laquelle la marque de conformité au Code de l'EUCROF de la CRO adhérente est en vigueur ou en cas de plainte contre la CRO, le COSUP a le droit de nommer un auditeur, conformément à la section 5.6.2, pour vérifier sur place l'application de la "déclaration d'exactitude et d'exhaustivité" et l'efficacité de la procédure d'adhésion et pour s'assurer que la documentation nécessaire est correctement mise à jour ou conservée.

5.5.6 Niveau 2 : évaluation par des Tiers

Cette procédure requiert un audit sur site de la CRO candidate ("procédure de niveau 2"). Cette évaluation sur place ne peut être effectuée que par un ou plusieurs auditeurs (leur nombre dépendant de la taille de la CRO candidate) sélectionnés et mandatés par le COSUP au sein du panel d'auditeurs.

Les principales étapes de la procédure de niveau 2 sont les suivantes :

1 La CRO candidate doit enregistrer sa candidature sur le site internet de l'EUCROF et compléter le pack de conformité qui comprend (a) le "profil de l'organisation" et (b) le "questionnaire de conformité" également utilisé pour la "procédure de niveau 1".

2 Ce pack de conformité préliminaire est examiné par le Responsable des Risques et de la Conformité en ce qui concerne (a) l'éligibilité et (b) l'exhaustivité et transmis au COSUP avec le rapport d'examen du Responsable des Risques et de la Conformité.

3 Le COSUP désigne alors un ou plusieurs auditeurs du panel d'auditeurs conformément aux procédures opérationnelles applicables définies par le COSUP.

4 Après confirmation, l'auditeur établira un devis sur la base de la documentation transmise. Ce devis doit être approuvé par écrit par la CRO candidate. Après approbation, le nom et le bref CV de l'auditeur seront transmis à la CRO candidate. L'auditeur reçoit du COSUP une instruction écrite pour effectuer l'audit correspondant.

5 L'auditeur organise et réalise alors son audit conformément aux conditions définies à la section 5.4.3 du présent Code et fournit le rapport correspondant avec sa recommandation au Responsable des Risques et de la Conformité et au COSUP sur l'approbation, l'approbation conditionnelle, ou le rejet. .

6 Le Responsable des Risques et de la Conformité peut alors demander des éclaircissements à l'auditeur. Une fois toutes les clarifications obtenues, le Responsable des Risques et de la Conformité prépare le rapport d'examen et transmet au COSUP l'ensemble de la documentation finale d'audit pour insertion dans l'ordre du jour d'une prochaine réunion du COSUP qui prendra la décision finale de valider ou non l'adhésion de la CRO candidate.

7 La décision sera communiquée à la CRO candidate conformément à la section 5.5.2.

5.5.7 Conditions d'utilisation des marques de conformité

L'EUCROF élaborera des marques de conformité officielles au Code de l'EUCROF pour chaque niveau. Ces marques de conformité au Code de l'EUCROF ne pourront être utilisées que par les CROs inscrites au registre public.

Les règles détaillées d'utilisation de ces marques de conformité au Code de l'EUCROF seront élaborées dans un document d'orientation validé par le COSUP et l'EUCROF.

L'utilisation abusive ainsi que la violation des conditions susmentionnées constituent une infraction au Code et peuvent donner lieu, à la discrétion du COSUP, à des amendes ou à des pénalités.

Si, après avoir été vérifié conforme par le COSUP, un litige concernant la non-conformité d'une CRO adhérente survient, l'utilisation de la marque de conformité au Code de l'EUCROF par la CRO doit être suspendue jusqu'à ce que les procédures de réclamation visées au point 5.7 aboutissent à une résolution. Après avoir reçu une décision finale de non-conformité au Code, la CRO doit immédiatement cesser d'utiliser la marque de conformité au Code de l'EUCROF.

5.6 Suivi et mise en œuvre

5.6.1 Validité de l'adhésion

Les décisions du COSUP de déclarer une CRO adhérente au Code ont une durée de validité de 3 ans à compter de la date de la décision. Avant la fin de chaque période de trois ans, la CRO adhérente doit demander le renouvellement de son adhésion au Code en suivant les mêmes procédures que celles décrites à la section 5.5. Si une CRO décide de ne pas poursuivre son adhésion, elle notifie formellement au COSUP son intention de se retirer de l'adhésion en utilisant le mécanisme de révocation publié par la COSUP. Si aucune notification d'intention de retrait ou de renouvellement n'a été reçue, le COSUP supprime la CRO du registre public conformément au document d'orientation visé à la section 5.5.7.

5.6.2 Contrôle

Au cours d'une période approuvée de trois ans, la conformité de toute CRO qui a été déclarée comme adhérant au Code est contrôlée par le COSUP une fois tous les douze mois et à tout moment en cas de :

a) Non-conformités majeures signalées ou non-conformités mineures répétées ;

b) Une plainte déposée par une personne concernée ou toute autre partie prenante intéressée ;

c) Changements significatifs survenant chez la CRO adhérente ; ou

d) En réaction à un article de presse défavorable ou à un retour d'information anonyme concernant une CRO figurant dans le registre public comme adhérant au Code.

Ce contrôle est effectué par un auditeur conformément à la procédure de contrôle de la conformité approuvée par le COSUP. Cette procédure de contrôle de la conformité et ses modifications éventuelles sont mises à la disposition du public sur le site internet de l'EUCROF. La décision finale concernant les activités de contrôle visant à déterminer la conformité ou la non-conformité d'une CRO adhérente et la responsabilité de la mise en œuvre qui en découle sont prises par le COSUP sur la base de l'audit/du contrôle effectué par les auditeurs.

Le suivi annuel intermédiaire se concentre sur les points d'amélioration listés lors des audits précédents ou sur les non-conformités identifiées lors des audits internes réalisés par l'entreprise adhérente elle-même dans le cadre de son Système de Management de la Sécurité de l'Information (SMSI). En outre, l'auditeur effectue des audits supplémentaires sur la base de sa connaissance de l'entreprise et d'une approche par échantillonnage. Nonobstant ce qui précède, la CRO adhérente doit se conformer à toutes les exigences du Code à tout moment et le COSUP peut à tout moment procéder à une évaluation complète.

5.6.3 Application de la loi

Si le COSUP a connaissance d'une non-conformité d'une CRO adhérente, le COSUP peut exiger de la CRO qu'elle prenne des mesures spécifiques pour cesser toute nouvelle infraction et adopter des mesures correctives dans un délai défini par le COSUP. Si ces mesures ne sont pas adoptées dans ce délai défini, la marque de conformité de la CRO adhérente au Code de l'EUCROF est suspendue. Le COSUP prend les mesures appropriées en ce qui concerne les sanctions et les mesures correctives conformément à la section 5.8.

En cas de révocation de la décision de conformité d'une CRO, le COSUP : a) en informe sans délai l'autorité de contrôle compétente et b) retire immédiatement la CRO concernée du registre public. La CRO cesse immédiatement de faire référence au Code ou à la marque de conformité au Code de l'EUCROF dans toute documentation ou publication, y compris sur son site internet.

5.7 Traitement des plaintes et procédures

5.7.1 Plaintes des CROs contre les décisions du COSUP

Les CROs peuvent déposer une plainte contre toute décision prise par le COSUP.

Les plaintes ou les recours contre le rejet de la candidature d'une CRO candidate dans le cadre de la procédure de niveau 1 ou de la procédure de niveau 2 sont adressés au Responsable des Risques et de la Conformité par le biais du site internet de l'EUCROF. Le COSUP est informé de la réception de la plainte dans un délai de deux jours ouvrables.

Le Responsable des Risques et de la Conformité examine la plainte ou l'appel et rédige un rapport d'examen dans les deux semaines suivant la réception de la plainte ou de l'appel. Au cours de cette phase, le Responsable des Risques et de la Conformité peut demander des éclaircissements supplémentaires à la CRO concernée et vérifier si la procédure de niveau 2 a été suivie. Le rapport d'examen ainsi que la plainte ou l'appel initial et toute information supplémentaire éventuelle fournie par la CRO à la demande du Responsable des Risques et de la Conformité sont ensuite transmis au COSUP et la question est inscrite à l'ordre du jour de la prochaine réunion du COSUP.

Le COSUP peut alors prendre la décision qu'elle juge la plus judicieuse, notamment accepter l'appel de la CRO concernée, demander des preuves supplémentaires de conformité, lancer une nouvelle procédure de vérification de la conformité ou confirmer le rejet antérieur.

5.7.2 Plaintes contre toute CRO adhérente

Si une partie prenante intéressée a des réserves concernant la conformité d'une CRO aux exigences du présent Code, cette personne est encouragée à contacter d'abord la CRO afin d'obtenir une solution mutuellement satisfaisante. Toutefois, la partie prenante intéressée peut directement déposer une plainte auprès du COSUP, sans contacter la CRO concernée.

Une telle plainte peut être déposée par toute partie, qu'elle soit ou non cliente de la CRO concernée, en son nom propre ou de manière anonyme sur le site internet de l'EUCROF.

Le COSUP examine la plainte, demande à la CRO de fournir toute information pertinente aux fins de l'établissement des faits, applique la procédure de contrôle de la conformité décrite au point 5.6.2 et entame une procédure de traitement des plaintes afin de déterminer si la plainte était justifiée. Si le COSUP conclut que la plainte était justifiée, elle prend les mesures appropriées pour mettre fin à toute nouvelle non-conformité de la CRO adhérente.

Les plaintes sont investiguées et résolues par le COSUP rapidement et dans un délai d'un mois, prolongeable de deux mois supplémentaires en tenant compte de la complexité de la plainte, de la gravité de la plainte et du niveau de risque de la plainte (en particulier l'impact sur la/les Personne(s) concernée(s)), comme spécifié dans la procédure de contrôle de conformité ou dans toute autre documentation appropriée.

Le COSUP décide des sanctions et des remèdes possibles conformément aux sanctions et aux remèdes prévus par le présent Code.

5.7.3 Coûts et honoraires liés aux plaintes

5.7.3.1 Coûts pour les plaignants

En règle générale, les plaintes peuvent être déposées sans frais pour le plaignant. Toutefois, le COSUP peut définir des coûts pour les plaignants, le cas échéant, afin d'éviter des abus potentiels dus à des plaintes manifestement infondées ou excessives, en particulier si elles sont récurrentes.

5.7.3.2 Coûts pour les CROs

Les coûts supplémentaires liés à toute plainte confirmée concernant une CRO adhérente sont à la charge de la CRO concernée ; ces coûts supplémentaires peuvent inclure les dépenses liées à des audits supplémentaires sur place ou à l'examen du dossier de plainte par un expert externe afin d'étayer la plainte.

Si cela est considéré comme justifié pour maintenir des opérations financières durables, le COSUP a la pleine capacité de proposer l'inclusion dans son budget annuel de frais supplémentaires pour le traitement des

plaintes. Dans ce cas, lorsque le budget annuel est approuvé par l'Assemblée Générale de l'EUCROF, ces frais supplémentaires sont rendus publics et connus de toutes les CROs adhérentes.

5.8 Sanctions, voies de recours et notification à l'Autorité de contrôle

Sans préjudice des tâches et des pouvoirs de l'autorité de contrôle compétente et des dispositions du chapitre VIII du RGPD, le COSUP prend les mesures appropriées en matière de sanctions et de recours à l'encontre de toute CRO adhérente qui se révèle non conforme aux exigences du présent Code ou qui rejette la coopération avec le COSUP dans l'accomplissement approprié de leurs tâches en vertu du présent code et du RGPD.

5.8.1 Sanctions et recours

Une CRO adhérente qui, après investigation conformément aux procédures de la section 5.6.2 et de la section 5.7.2, est constatée comme n'ayant pas respecté une exigence du Code, fait l'objet de sanctions et de mesures correctives appropriées. Le COSUP prend en compte les aspects suivants pour évaluer la pertinence de chaque action :

- Gravité de la non-conformité au regard de l'impact potentiel sur le niveau de protection des données liées aux données à caractère personnel traitées, y compris l'impact potentiel sur les libertés et les droits des personnes concernées.
- Responsabilité de la CRO selon qu'elle a intentionnellement ignoré les exigences du Code ou qu'elle les a mal interprétées par négligence.
- Fréquence de la non-conformité ; s'agit-il de la première infraction ou y a-t-il eu des incidents similaires auparavant.

Sur la base des critères susmentionnés, le COSUP impose des sanctions et des recours qui peuvent être l'un des éléments suivants ou une combinaison de ceux-ci :

- Réprimande non publique mais formelle.
- Annonce publique de la non-conformité et de la réprimande formelle qui s'ensuit, y compris les faits et le raisonnement.
- La révocation temporaire ou permanente de la CRO du registre public et la révocation connexe de leur droit d'utiliser une marque de conformité au Code de l'EUCROF.

5.8.2 Lignes directrices concernant les sanctions et les voies de recours

Afin de garantir la comparabilité et la cohérence des sanctions et des mesures correctives imposées aux CROs, le COSUP élaborera et mettra en œuvre des lignes directrices régissant les sanctions et les mesures correctives ou les fourchettes de sanctions à imposer aux CROs.

Ces lignes directrices sont rédigées, approuvées et fréquemment révisées par le COSUP en tenant compte de l'expérience pratique du COSUP en ce qui concerne les cas de non-conformité de la part des CRO adhérentes.

Les lignes directrices énumèrent et documentent, à l'aide d'exemples, tous les types de non-conformité envisagés ainsi que les sanctions et/ou les mesures correctives correspondantes à prévoir. La détermination des sanctions et des recours doit prendre en compte tout aspect utile afin d'évaluer l'adéquation d'une sanction ou d'un recours, tel que défini au point 5.8.1.

Le COSUP peut à tout moment s'écarter des lignes directrices disponibles, à condition que le COSUP mentionne explicitement son écart dans sa décision et qu'elle motive de manière appropriée les raisons pour lesquelles cet écart a été jugé nécessaire. Une telle décision entraîne une révision des lignes directrices.

5.8.3 Notification et coopération avec les autorités de contrôle par le COSUP

Sans préjudice de l'article 41, paragraphe 4, du RGPD, le COSUP notifie de manière proactive et en temps utile à l'autorité de contrôle compétente les sanctions et les mesures correctives imposées aux CROs et les raisons pour lesquelles elles ont été prises, y compris les réprimandes non publiques mais formelles.

Si une autorité de contrôle indique au COSUP qu'elle est préoccupée par le fait que les mesures prises par le COSUP ne correspondent pas à ce que les autorités de contrôle considèrent comme une action appropriée, le COSUP tiendra compte de ce retour d'information pour toute décision future.

Dans tous les cas, le COSUP coopère avec les autorités de contrôle en fournissant des informations complètes sur les circonstances à l'origine de la sanction et sur la justification des décisions prises par le COSUP. Le COSUP répond rapidement à toute demande d'informations complémentaires et met en œuvre les recommandations ou exigences et les actions supplémentaires que les autorités de contrôle jugent nécessaires.

5.9 Finances

5.9.1 Gestion financière

Le COSUP est responsable de la gestion de ses budgets annuels de la manière la plus appropriée. Il incombe au président d'organiser la gestion financière de la manière la plus efficace possible. Cette tâche comprend :

- Élaborer un budget annuel prévisionnel du COSUP pour l'année à venir et le soumettre à l'approbation du COSUP.
- Rendre compte de l'exécution du budget annuel de l'année écoulée et faire approuver l'état annuel par le COSUP.
- Fournir des informations financières à l'Assemblée Générale de l'EUCROF afin de permettre à l'EUCROF de remplir ses propres rapports financiers concernant l'argent qu'elle a fourni au COSUP.
- Ordonner tous les paiements requis en relation avec l'exécution du budget de l'année en cours et dans le cadre du budget approuvé.

Sur proposition du Président, le COSUP peut désigner un de ses membres pour exécuter les tâches susmentionnées au nom et sous la responsabilité du Président. Cette désignation est soumise au vote du COSUP.

Le budget annuel du COSUP couvre les coûts du secrétariat, du Responsable des Risques et de la Conformité, du panel d'auditeurs, de la plateforme informatique et des activités du COSUP.

5.9.2 Dépenses éligibles du COSUP

Les dépenses du COSUP qui sont éligibles sont les suivantes :

a. Une indemnité sera allouée aux membres pour leur participation aux activités du COSUP. Le montant de cette indemnité dépend (a) du rôle du membre - Président, Vice-Président, membre ordinaire - et (b) du type de réunion (réunion physique ou téléconférence).

b. Les frais de déplacement et d'hébergement encourus dans l'exercice de leurs fonctions sont remboursés aux membres sur la base de justificatifs et conformément aux conditions définies dans la politique financière de l'EUCROF.

c. Toute autre exigence nécessaire au bon fonctionnement du COSUP, telle que la location de salles de réunion, les moyens techniques (moyens de téléconférence...), l'achat de rapports sur des sujets d'intérêt, etc...

5.9.3 Cotisations annuelles perçues par les membres de l'EUCROF et les CROs non-membres adhérentes

Tous les coûts récurrents inclus dans le budget annuel géré par le COSUP sont couverts par les cotisations annuelles perçues par les membres de l'EUCROF ainsi que par les CROs adhérentes non-membres.

Pour les organisations membres d'EUCROF, cette cotisation est incluse dans leur cotisation annuelle et est approuvée chaque année par l'Assemblée Générale sur la base du budget annuel proposé par le Président du COSUP.

Le montant de la cotisation annuelle demandée aux organisations non-membres souhaitant adhérer au Code peut être différent de celui demandé aux organisations affiliées. Le montant de la cotisation annuelle pour les

organisations non-membres est proposé par le Président dans le cadre du budget annuel et approuvé chaque année par l'Assemblée Générale. Cette cotisation annuelle est publiée sur le site internet de l'EUCROF.

Conformément au point 5.4.5 et au point 5.7.3.2 du présent Code, les coûts liés aux audits et/ou au traitement des plaintes seront directement imputés à l'organisation concernée, en plus de la cotisation annuelle normale.

5.9.4 Contrôle et publication

Les comptes du COSUP seront intégrés dans l'état annuel des comptes de l'EUCROF sous des lignes analytiques distinctes et seront accessibles au public.

Le président du COSUP se concerte en tant que de besoin avec le trésorier de l'EUCROF pour publier en temps utile des rapports sur le budget annuel de l'année écoulée.

Les comptes du COSUP seront soumis aux mêmes règles de contrôle et d'approbation que le budget général de l'EUCROF.

5.10 Examen et mise à jour du code

Le porteur du Code procède à un examen périodique du contenu du Code de conduite, tous les deux (2) ans, afin de pouvoir l'amender et y intégrer les modifications nécessaires pour faciliter le respect des règles de protection des données dans le domaine de la recherche clinique, dans un environnement en constante évolution. Ces révisions périodiques sont sans préjudice d'une éventuelle révision du Code chaque fois que l'exigent de nouveaux développements législatifs ou jurisprudentiels ou des évolutions technologiques.

Le porteur du Code détermine si une révision est exigée en dehors du cycle de révision régulier et peut, à sa discrétion, consulter le COSUP et l'Autorité de contrôle compétente pour décider si une révision est requise. Dans tous les cas, le porteur du Code est responsable des modifications apportées au Code. Le Code modifié est examiné par l'Autorité de contrôle compétente et, lorsque les modifications sont substantielles, il peut être nécessaire de le soumettre à une nouvelle approbation conformément aux lignes directrices du Contrôleur Européen de la Protection des Données. Lorsque les modifications sont de nature administrative, par exemple pour corriger des adresses, des problèmes d'orthographe ou des références croisées, elles peuvent être publiées sans l'approbation de l'Autorité de contrôle compétente.

Le porteur du Code publie toute nouvelle version approuvée du Code sur le site Internet de l'EUCROF au moins cinq (5) jours ouvrables après son approbation et envoie une notification à tous les adhérents et candidats au Code dans les cinq (5) jours ouvrables suivant la publication de la nouvelle version. Le porteur du Code fournit à la fois la nouvelle version du Code avec un résumé des dernières modifications apportées et la ligne rouge montrant les modifications apportées afin de simplifier le processus d'examen pour les parties prenantes.

Toutes les CROs adhérentes disposent de 60 jours à compter de la date d'entrée en vigueur de la nouvelle version pour mettre en œuvre les changements. Après cette période de transition de 60 jours, l'auditeur du COSUP effectue des contrôles ponctuels auprès des CROs adhérentes dont la marque de conformité au Code de l'EUCROF ne doit pas être renouvelée dans les 6 mois suivant la date d'entrée en vigueur, afin de vérifier que les CROs adhérentes sont passées à la nouvelle version. Le processus de renouvellement suivant pour la CRO adhérente sera basée sur la version en vigueur et un écart sera considéré si la CRO n'a pas mis en œuvre la version actuelle du Code.

Enfin, le Code n'est pas un instrument statique, mais un instrument qui peut subir des modifications successives pour l'adapter aux nouveaux critères d'interprétation des décisions des Autorités de contrôle, aux derniers précédents jurisprudentiels et aux besoins qui peuvent être soulevés par les entités adhérentes à la suite du développement technologique et scientifique dans les domaines réglementés par le Code.

Niveau de révision	Date d'entrée en vigueur	Justification de la révision
Version 1.0	TBD	Nouveau code

Annexe 1 Liste des autorités de contrôle concernées

(1) Autriche	Österreichische Datenschutzbehörde (Office autrichien de protection des données) Barichgasse 40-42 1030 Wien https://www.dsb.gv.at/
(2) Belgique	Autorité de la protection des données Autorité de certification (APD-GBA) Rue de la Presse 35 - Drukpersstraat 35 1000 Bruxelles - Brussel https://www.autoriteprotectiondonnees.be/ https://www.gegevensbeschermingsautoriteit.be/
(3) Bulgarie	Commission pour la protection des données à caractère personnel 2, Prof. Tsvetan Lazarov blvd. Sofia 1592 https://www.cpdp.bg/
(4) Croatie	Agence croate de protection des données à caractère personnel Martićeva 14 10000 Zagreb http://www.azop.hr/
(5) Chypre	Commissaire (membre des données à caractère personnel CNIL) 1 rue Iasonos, 1082 Nicosie Boîte postale 23378, CY-1682 Nicosie http://www.dataprotection.gov.cy/
(6) République tchèque	Office pour la protection des données à caractère personnel Pplk. Sochora 27 170 00 Prague 7 http://www.uoou.cz/
(7) Danemark	Datatilsynet Carl Jacobsens Vej 35, 2500 Valby http://www.datatilsynet.dk/
(8) Estonie	Inspection estonienne de la protection des données à caractère personnel (Andmekaitse Inspektsioon) Tatari 39 10134 Tallinn http://www.aki.ee/
(9) Finlande	Bureau du Médiateur pour la protection des données à caractère personnel Boîte postale 800 FIN-00521 Helsinki

http://www.tietosuoja.fi/en/

(10) France	Commission Nationale de l'Informatique et des Libertés - CNIL 3 Place de Fontenoy TSA 80715 - 75334 Paris, Cedex 07 https://www.cnil.fr/
(11) Allemagne	Autorité Fédérale Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Les députés fédéraux pour la protection des données et la liberté d'information) Husarenstraße 30 53117 Bonn http://www.bfdi.bund.de/ Autorités régionales («Land») La liste complète des autorités régionales peut être trouvée ici: https://www.datenschutzkonferenz-online.de/datenschutzaufsichtsbehoerden.html
(12) Grèce	Autorité hellénique de protection des données à caractère personnel Kifisias Av. 1-3, PC 11523 Ampelokipi Athènes http://www.dpa.gr/
(13) Hongrie	Autorité nationale hongroise pour la protection des données à caractère personnel et la liberté d'information Szilágyi Erzsébet fasor 22/C H-1125 Budapest http://www.naih.hu/
(14) Irlande	Protection des données à caractère personnel 21 Fitzwilliam Square Dublin 2 D02 RD28 Irlande http://www.dataprotection.ie/
(15) Italie	Garanties pour la protection des données à caractère personnel Piazza Venezia, 11 00187 Roma http://www.garanteprivacy.it/
(16) Lettonie	Inspection de l'État des données Blaumana str. 11/13-15 1011 Riga http://www.dvi.gov.lv/
(17) Lituanie	Inspection nationale de la protection des données à caractère personnel A. Juozapaviciaus str. 6 LT-09310 Vilnius http://www.ada.lt/

(18) Luxembourg	Commission Nationale pour la Protection des Données 1, avenue du Rock'n'Roll L-4361 Esch-sur-Alzette http://www.cnpd.lu/
(19) Malte	Commissariat (membre de la CNIL) de l'information et de la protection des données à caractère personnel Deuxième étage, Airways House High Street, Sliema SLM 1549 http://www.idpc.org.mt/
(20) Pays-Bas	Autoriteit Persoonsgegevens Bezuidenhoutseweg 30 Boîte postale 93374 2509 AJ Den Haag/The Hague https://autoriteitpersoonsgegevens.nl/nl
(21) Pologne	Urząd Ochrony Danych Osobowych (Office de protection des données à caractère personnel) ul. Stawki 2 00-193 Varsovie https://uodo.gov.pl/
(22) Portugal	Comissão Nacional de Protecção de Dados - CNPD Av. D. Carlos I, 134, 1º 1200-651 Lisboa http://www.cnpd.pt/
(23) Roumanie	L'Autorité de contrôle nationale pour le traitement des données à caractère personnel B-dul Magheru 28-30 Secteur 1, BUCUREŞTI http://www.dataprotection.ro/
(24) Slovaquie	Office pour la protection des données à caractère personnel de la République slovaque Hraničná 12 820 07 Bratislava 27 http://www.dataprotection.gov.sk/
(25) Slovénie	Commissaire (membre de la CNIL) Mme Mojca Prelesnik Dunajska 22 1000 Ljubljana https://www.ip-rs.si/
(26) Espagne	Agence espagnole de protection des données (AEPD) C/Jorge Juan, 6 28001 Madrid

https://www.aepd.es/

(27) Suède

Types de données
Drottninggatan 29
5ème étage
Boîte postale 8114
104 20 Stockholm
http://www.datainspektionen.se/

Annexe 2 Classes de services entrant dans le champ d'application du présent code

Pour chaque catégorie de service, un tableau donne un aperçu de l'objet, de la finalité, de la nature et de la durée du traitement, ainsi que des types de données à caractère personnel.

La durée du traitement mentionnée dans les tableaux n'a qu'une valeur indicative : c'est le responsable du traitement qui a la charge de la définir.

Certaines données à caractère personnel concernant le personnel du promoteur et le personnel de la CRO peuvent toujours être traitées par la CRO en tant que responsable du traitement dans le cadre de la communication commerciale pour la fourniture du service ; toutefois, ce traitement reste en dehors du champ d'application du présent Code, comme indiqué dans son champ d'application (voir section 1.9.2).

Lorsqu'il n'est pas envisagé de traiter des données à caractère personnel dans le cadre d'une catégorie de services particulière, il est indiqué "Non Applicable" (NA). Cela peut être le cas lorsque la catégorie de service est pertinente pour définir la manière dont les données à caractère personnel doivent être collectées et utilisées dans une autre catégorie de service, mais qu'il n'y aura pas de traitement de données à caractère personnel à ce stade ; par exemple (2) le formulaire éclairé et la notice d'information de l'ICF.

Les tableaux et leur contenu sont destinés à servir de guide général et ne constituent pas une liste exhaustive. Il est conseillé à chaque CRO d'interpréter sa situation particulière et, le cas échéant, des conclusions différentes peuvent être prises en compte dans le cadre de l'utilisation du présent Code et seront reflétées dans l'Accord relatif au traitement des données.

(1) Synopsis, protocole et conception du cahier d'observations

Ce premier processus de mise en place de l'étude concerne la conception du protocole de l'étude (qui définit la Finalité et les moyens, y compris la justification de la Collecte de données sensibles) et du cahier d'observations (qui identifie les données à collecter).

Objet du traitement :	Élaboration de lignes directrices (protocole), de plans de projet, de formulaires de collecte de données, y compris de cahiers d'observations.
Finalité du traitement :	Mise en place du cadre de preuves pour la prise en compte du respect de la vie privée dès la conception, y compris l'intégration des principes de minimisation des données, de limitation des finalités et de confidentialité.
Nature du traitement :	Le traitement des données à caractère personnel des sujets d'étude n'est pas envisagé.
Types de données à caractère personnel :	NA
Durée du traitement :	NA

(2) Dépliant d'information et de conception du formulaire éclairé

Désigne l'ensemble des activités menées pour concevoir l'information et/ou le formulaire de consentement éclairé (FCI) pour les sujets de l'étude, conformément au type d'étude et aux dispositions réglementaires applicables.

Objet du traitement :	Élaboration d'informations à l'intention des personnes participant à l'étude sur le traitement des données liées à l'étude.
Finalité du traitement :	Conformité avec le droit à l'information des sujets de l'étude.
Nature du traitement :	Le traitement des données à caractère personnel des sujets d'étude n'est pas envisagé.
Types de données à caractère personnel :	NA

Durée du traitement :	NA

(3) Sélection du site et contrat

Désigne toutes les activités liées à la sélection des Sites Investigateurs susceptibles de participer à une étude clinique, y compris dans le cadre d'une étude de faisabilité, jusqu'à la signature du contrat avec les Sites Investigateurs. Le service concerné peut être désigné par les termes "faisabilité du site", "identification du site" et "sélection de l'investigateur". Les CROs qui organisent des réunions investigateurs doivent se référer à la classe de service (23) Organisation de réunions investigateurs.

Objet du traitement :	Collecte (de données à caractère personnel) des professionnels de la santé.
Finalité du traitement :	Sélection de Professionnels de santé qualifiés et capables d'accomplir les tâches de l'investigateur ; évaluation de la compensation et de la rémunération.
Nature du traitement :	Collecte/obtention, transfert/transmission, stockage, analyse, suppression/destruction.
Types de données à caractère personnel :	Professionnels de santé : nom, prénom, sexe, date de naissance, signature, adresse postale, coordonnées électroniques et téléphoniques, coordonnées bancaires ; formation : qualification(s) ; vie professionnelle (notamment parcours professionnel, mode et type d'exercice, éléments nécessaires à l'évaluation des connaissances dont ils disposent pour mener la Recherche) ; le cas échéant, numéro d'inscription au registre partagé des Professionnels de santé ; rémunération totale et rémunération perçue ; participation à d'autres Études ; programmes de formation, performances.
Durée du traitement :	De la réunion de soutenance à l'achèvement des initiations de sites, l'identification des sites peut se poursuivre tout au long de l'étude.

(4) Collecte des données

Désigne toutes les activités réalisées par la CRO en rapport avec la Collecte (de données) nécessaire aux fins de la Recherche Clinique.

Objet du traitement :	Création des bases de données d'études cliniques pour mener des recherches.
Finalité du traitement :	Permettre la réalisation de l'objectif principal de la recherche ; identification (des personnes) en tant que sujets d'étude.
Nature du traitement :	Collecte/obtention, transfert/transmission, stockage, analyse.
Types de données à caractère personnel :	Sujets d'étude : données relatives à la santé ; photographies et/ou enregistrements vidéo et/ou vocaux ne permettant pas d'identifier les sujets de recherche, par exemple en masquant le visage, les yeux, les caractéristiques distinctives, sauf si ces caractéristiques sont strictement nécessaires aux fins de la recherche clinique, dates relatives à la conduite de la recherche, c'est-à-dire la date d'inscription et les dates de visite ; origine ethnique, si elle est scientifiquement justifiée et nécessaire pour se conformer aux objectifs de la recherche ; état civil ; niveau génétique strictement nécessaire pour se conformer aux objectifs ou aux finalités de la recherche, ne permettant pas une identification directe ou indirecte ; date d'inscription et dates de visite, la date d'inscription et les dates de visite ; l'origine ethnique, si elle est scientifiquement justifiée et nécessaire au respect des objectifs de l'étude ; les données génétiques strictement nécessaires au respect des objectifs ou des finalités de la recherche, ne permettant pas l'identification directe ou indirecte ; l'état civil ; le niveau d'éducation ; la catégorie

	socioprofessionnelle ; la vie professionnelle, par ex, exposition professionnelle ; affiliation à la sécurité sociale (à l'exclusion du numéro d'inscription au répertoire national d'identification des personnes physiques), assurance complémentaire (mutuelle, assurance privée) ; participation à d'autres recherches ou études, afin de garantir le respect des critères d'inclusion ; consommation de tabac, d'alcool et de drogues récréatives ; modes de vie et comportements, assistance (aide domestique, famille), exercice physique (intensité, fréquence, durée), régime alimentaire et habitudes alimentaires, loisirs ; mode de vie, par ex, urbain, semi-urbain, voyageur, sédentaire ; logement maison ou immeuble privé, étage, ascenseur, etc. ; vie sexuelle ; statut vital, etc.
Durée du traitement :	Présélection jusqu'à la fin de l'étude/le retrait de l'étude ou jusqu'à ce que le produit de l'étude reçoive une autorisation de mise sur le marché ou jusqu'à deux ans après la publication finale des résultats de la recherche ; ou, en l'absence de publication, jusqu'à ce que le rapport final de la recherche ait été signé.

4.1 Données Collecte (de données) directement auprès des personnes concernées/procurées

Désigne tous les processus où les données sont collectées directement par la personne concernée elle-même et/ou un mandataire.

Exemples :

- Données collectées par la CRO au moyen d'entretiens en face à face, en ligne, par téléphone, à l'aide d'enregistrements et de transcriptions électroniques ou sur papier.
- Données collectées par la CRO via des plateformes téléphoniques : questionnaires téléphoniques (PRO) à des fins diverses, notamment la qualité de vie, l'évaluation pharmacoéconomique, les enquêtes sur la charge de morbidité, la satisfaction à l'égard du traitement, la tolérabilité, les questionnaires de dépistage pour détecter les problèmes de sécurité, l'évolution des symptômes, l'efficacité des stratégies d'atténuation des risques telles que les programmes d'éducation des patients, la présélection en vue de l'inclusion dans une étude. Ces évaluations peuvent être réalisées indépendamment des investigateurs (contrôle du biais d'influence et donc amélioration de la qualité des données ; pas de valeur ajoutée à ce que l'évaluation soit réalisée par un professionnel de la santé) ou en collaboration avec les investigateurs, par exemple, un événement d'intérêt détecté par un contact déclenchera une alerte pour que l'investigateur ou le sujet de l'étude prenne contact avec le Site Investigateur.
- Données collectées par la CRO auprès des patients en conditions réelles par le biais d'ePRO, d'eCOA ou d'autres supports électroniques (EDC, smartphone, tablette) ou sur papier.
- Données collectées dans le cadre d'une procédure et d'outils de consentement électronique.

4.2 Collecte des données par les Professionnels de santé au moyen du cahier d'observations (papier ou électronique)

Il s'agit de tous les processus au cours desquels les données sont collectées par les professionnels de santé des sites Investigateurs au moyen de cahiers d'observations.

4.3 Collecte (de données) à partir d'autres sources de données

Il s'agit de tous les processus dans lesquels les données sont collectées à partir de sources externes : Dossiers médicaux électroniques (DME), registres nationaux, laboratoires locaux, etc.

Ce type de Collecte (de données) s'observe notamment dans le cadre des études en vie réelle.

(5) Contrôle

Il s'agit de toutes les activités réalisées par la CRO dans le cadre du monitoring de l'étude. Le processus de monitoring s'efforce de remplir trois Finalités :

- Protéger les droits et le bien-être des sujets d'étude humains,

- Mener l'étude en conformité avec le protocole, les BPC ou toute autre norme applicable et les exigences réglementaires en vigueur,
- Vérifier l'exactitude et l'exhaustivité des données de l'étude clinique.

Objet du traitement :	Comparer les enregistrements sources et les formulaires de Collecte (de données) remplis, s'assurer que le formulaire de consentement éclairé est correctement rempli et stocké, établir des rapports sur la sécurité.
Finalité du traitement :	Vérification de l'exactitude du transfert des données des dossiers sources vers les formulaires de Collecte (de données) de l'étude, de l'autorisation appropriée au traitement et de la participation.
Nature du traitement :	Collecte/obtention, examen, accès, transfert/transmission, analyse, stockage, suppression/destruction.
Types de données à caractère personnel :	Sujets de l'étude : les mêmes que pour (4) Collecte des données.
Durée du traitement :	Depuis l'enrôlement du premier patient jusqu'au verrouillage de la base de données du cahier d'observations.

Les activités de monitoring sont généralement menées selon trois approches différentes, décrites ci-dessous.

5.1 Monitoring sur site

Lors des visites de monitoring sur site, l'Attaché de Recherche Clinique (ARC) de l'étude est censé vérifier, au minimum, la documentation relative au consentement éclairé et le dossier médical du patient afin d'évaluer l'exactitude et l'exhaustivité des données de l'étude clinique collectées. Au cours de ces visites, l'ARC de l'étude a accès aux données directement identifiables des personnes concernées. Cette activité de traitement des données requiert donc une attention particulière afin de protéger le sujet de l'étude contre toute divulgation de ses données sensibles.

5.2 Monitoring à distance (également connue sous le nom de vérification à distance des données [SDV])

Le monitoring à distance est une évaluation effectuée par des ARCs dans un lieu autre que les Sites Investigateurs, dans le but de sélectionner, d'initier, de contrôler ou de fermer des Sites. Elle comprend des activités de surveillance axées sur la vérification des données critiques, y compris les données sources, et des processus critiques.

Le monitoring à distance utilise intensivement des environnements virtuels où les données/informations peuvent être collectées par le biais d'entretiens/de questions et/ou de documents sources pouvant être téléchargés par le personnel du Site Investigateur. Le monitoring à distance doit être conforme aux exigences propres à chaque pays et est soumis à l'autorisation/accord des Sites Investigateurs.

Le promoteur doit justifier et documenter la justification et les processus à suivre pour l'utilisation du monitoring à distance en général et en particulier pour la vérification à distance des données sources. En outre, les lignes directrices européennes et nationales doivent être suivies, et les CROs doivent se référer aux lignes directrices du Contrôleur Européen de la Protection des Données et aux normes nationales publiées par les autorités de contrôle, ainsi qu'à d'autres lignes directrices européennes, telles que celles publiées par l'Agence Européenne des Médicaments[24] .

Le promoteur est responsable de la décision d'effectuer un monitoring à distance. La CRO est en mesure de fournir des recommandations sur l'opportunité de mettre en place le monitoring à distance. Étant donné que, dans la plupart des cas, les documents quittent le Site Investigateur, des mesures de sécurité supplémentaires doivent être spécifiées et organisées.

5.3 Monitoring centralisé (data management)

Le monitoring centralisé est une activité axée sur les données, dans le cadre de laquelle les gestionnaires de données effectuent des contrôles sur les données et fournissent des indicateurs et une analyse

[24] Document de recommandation sur les éléments décentralisés dans les essais cliniques par l'EMA, Version 01, 13 décembre 2022

approfondie des données aux moniteurs de l'étude. Les ARCs effectuent ensuite un contrôle (sur site et/ou à distance, si cela se justifie) pour résoudre les problèmes détectés.

(6) Suivi médical

Les services de surveillance médicale varient en fonction de la conception de l'étude et de la classification réglementaire. La surveillance médicale est réglementée pour les études cliniques.

Ces services peuvent comprendre les activités suivantes :

- Participation aux comités de pilotage de l'étude et intégration de l'expertise le cas échéant ;
- Élaboration et/ou révision du protocole et des documents de l'étude (initiaux et amendements) ;
- Participation à l'évaluation de la faisabilité de l'étude et à la sélection du Site Investigateur ;
- Formation des parties prenantes de l'étude, y compris la participation aux réunions investigateurs en mettant l'accent sur l'IMP et les aspects médicaux du protocole ;
- Résoudre les problèmes quotidiens et fournir des conseils médicaux à l'équipe de projet sur des questions liées à l'étude, par exemple des questions spécifiques au site pour clarifier le protocole, remplir le cahier d'observations, des questions de gestion liées à la sécurité ; pour les études interventionnelles, vérifier l'éligibilité des patients conformément au protocole et examiner les écarts par rapport au protocole.
- Surveillance étroite de la base de données de l'étude clinique du point de vue de la sécurité.
- Fournir des informations médicales sur les données de sécurité et les descriptions de cas.
- Examiner la liste des données et le codage pour le sens médical.
- Examiner et commenter l'analyse et les résultats des données de l'étude clinique (Plan d'analyse statistique (PAS), Rapport d'étude clinique (CSR), publications).

Objet du traitement :	Conformité avec les exigences réglementaires, évaluation de l'admissibilité des sujets de l'étude à participer ou à continuer à participer à l'étude.
Finalité du traitement :	Mission de contrôle de la gestion appropriée des risques liés à la santé, analyse de l'impact du produit expérimental sur le bien-être des sujets de l'étude.
Nature du traitement :	Collecte/obtention, transfert/transmission, analyse, stockage.
Types de données à caractère personnel :	Sujets de l'étude : les mêmes que pour (4) Collecte des données.
Durée du traitement :	Inscription du premier patient, nettoyage des bases de données de surveillance de la sécurité et verrouillage de la base de données des cahiers d'observations/transfert du fichier principal de l'essai.

(7) Pharmacovigilance (PV) et rapports de sécurité

Les CROs peuvent fournir un large éventail de services contribuant à la sécurité des médicaments et des dispositifs médicaux. Ces services sont fournis dans le cadre de la post-commercialisation (système de notification spontanée en dehors d'une étude et autres services tels que l'analyse systématique de la littérature et la détection des signaux) et/ou dans le cadre d'études ou d'autres systèmes organisés de collecte de données qui ne sont pas considérés comme des études cliniques (collecte sollicitée d'informations relatives à la sécurité).

Les procédures typiques gérées par les équipes PV dans les études sont les suivantes :

- des conseils sur les événements indésirables (EI) recueillis au cours de l'étude et les règles de notification par le Site Investigateur à l'équipe PV ;
- la gestion des rapports de sécurité des cas individuels (y compris l'accusé de réception des rapports d'EI individuels, le tri des cas pour éviter les doublons, l'enregistrement dans la base de données de

sécurité, le contrôle de la qualité des rapports d'EI et l'interrogation, l'évaluation du lien de causalité et la rédaction de l'exposé des faits) ; et

- Soumission des cas valables aux autorités compétentes, le cas échéant.

Ces activités sont très réglementées. Elles exigent l'utilisation d'une base de données indépendante de la base de données de l'étude clinique, permettant une gestion correcte des cas et la soumission électronique des cas valides aux bases de données régionales (typiquement, EudraVigilance dans l'UE).

Outre la gestion et la soumission de cas individuels, la pharmacovigilance exige la production de rapports agrégés périodiques (rapport actualisé de pharmacovigilance pour les produits en développement, Rapport périodique actualisé de sécurité). Le traitement des cas peut nécessiter des contacts nominatifs directs avec les déclarants (consommateurs et professionnels de la santé), mais la soumission aux autorités est gérée de manière anonyme.

Objet du traitement :	Identique à (6) Suivi médical.
Finalité du traitement :	
Nature du traitement :	
Types de données à caractère personnel :	
Durée du traitement :	

(8) Services directs aux patients (DtP)

Services complémentaires aux patients qui nécessiteront le traitement des données administratives d'identification des Personnes concernées par l'étude (nom, prénom, adresse postale, coordonnées électroniques et téléphoniques, coordonnées bancaires).

Exemples de services DtP pouvant être fournis par une CRO :

- L'organisation des voyages, y compris l'avion, le train, le taxi, les transports spéciaux, par exemple pour les patients atteints de la maladie de Crohn, les réservations d'hébergement et le remboursement des frais de transport pour les sujets de l'étude et/ou le versement d'indemnités ;
- Suivi des personnes concernées comme spécifié dans le protocole de recherche, par exemple, envoi d'un message texte [SMS] pour répondre à un questionnaire en ligne, activation d'un compte informatique pour utiliser une application liée ;
- Engagement des patients dans l'étude, par exemple, une CRO emploie une plateforme en ligne ou autre par laquelle les sujets potentiels de l'étude peuvent recevoir une référence au site médical le plus proche ; le site médical effectuera l'évaluation finale de l'éligibilité et l'inscription ;
- Livraison des produits de santé et des équipements, par exemple des appareils de dialyse ;
- Livraison et collecte à domicile des échantillons nécessaires à la recherche ;
- Services de soins infirmiers à domicile ;
- Restauration, par exemple pour les patients anorexiques nécessitant un régime spécial ;
- Services d'accompagnement lors des visites des patients à l'hôpital, y compris le passage rapide dans les files d'attente de l'hôpital, la fourniture de nourriture (restrictions diététiques spéciales, suite au retrait d'échantillons) ;
- Soutien psychologique par des professionnels, explications supplémentaires pour une étude (organisation ; utilisation d'un appareil) ;
- Entretiens avec les patients, par exemple fonctions de défense, exigeant une interaction avec les patients et les familles, par exemple E-produits permettant une interaction directe avec le patient via des plateformes en ligne ou des systèmes de messagerie électronique, y compris les résultats électroniques rapportés par les patients (ePRO) ; et
- Plates-formes téléphoniques permettant une interaction directe avec le patient ; questionnaires téléphoniques à des fins variées, notamment les PROs, les questionnaires de qualité de vie (QoL), l'évaluation pharmacoéconomique, etc.

Objet du traitement :	Communication pour la fourniture du service.
Finalité du traitement :	Fournir un soutien lié aux activités administratives qui sont nécessaires ou complémentaires à la recherche et qui vont au-delà de l'objectif essentiel de la recherche.
Nature du traitement :	Collecte/obtention, transfert/transmission, stockage, désidentification -(pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données), suppression/destruction.
Types de données à caractère personnel :	Dépend du type de service et impliquera une combinaison de données minimales sur la santé, par exemple le nom de la maladie, des informations générales sur l'état de santé spécifique de la personne, avec des données d'identification des Identifiants, par exemple le nom, le prénom, l'adresse postale, l'adresse électronique, les coordonnées bancaires, les services de transport, la localisation, les coûts de remboursement, etc.
Durée du traitement :	Les données de la Personne concernée sont reçues jusqu'à la fin de la prestation du service, les données d'identification étant alors supprimées ; la durée de conservation des données agrégées à des fins de responsabilité financière est définie par la Loi applicable (droit national applicable).

(9) Gestion des données

Se réfère aux activités suivantes :

- Élaboration d'un plan de gestion des données (Plan de Data Management) avant le début des activités de gestion des données, afin de décrire les processus utilisés pour gérer les données tout au long de l'étude.
- Processus de développement de systèmes de Collecte de données pour les systèmes papier, électroniques et hybrides ; cela couvre la gestion du logiciel de collecte des données (EDC) depuis la configuration, la maintenance et le contrôle des changements pendant la phase de production.
- Contrôle de la qualité de la base de données pour les documents papier (y compris la définition de l'échantillon, des données et des variables à vérifier et du seuil acceptable, ainsi que des mesures à prendre en fonction des résultats).
- Processus continu de nettoyage des données au cours de l'étude, depuis les premières données saisies jusqu'au verrouillage final de la base de données. Pour ce faire, on utilisera les contrôles de vérification du programme, l'examen des listes de données, l'examen médical, l'examen de la qualité et la vérification des données sources. Ce processus peut inclure un rapprochement avec des données externes.
- Processus de codage des données pour permettre le codage des données médicales reçues via la base de données médicales conformément aux directives de codage définies ; cela comprendra le processus de codage automatique et manuel ainsi que l'examen des rapports de codage.
- Processus de rapprochement de la base de données des événements de sécurité pour rapprocher les principales variables des données des événements de sécurité stockées dans la base de données clinique de l'étude et dans la base de données de sécurité/pharmacovigilance.
- Examen des données (intermédiaire, final) : la qualité des données est évaluée et des décisions générales sont prises pour garantir que les données transmises pour l'analyse auront le niveau de qualité approprié.
- Processus de verrouillage et de déverrouillage de la base de données pour les bases de données provisoires et finales de l'étude afin de restreindre l'accès à la base de données et d'éviter toute modification non autorisée de la base de données propre avant les analyses. Ce processus comprend l'extraction de la base de données dans un emplacement spécifique garantissant un accès en lecture seule, mais aussi l'absence de modification entre la copie des fichiers extraits et la suppression des droits d'accès à la base de données.

- Processus de transfert de données (importation et exportation), y compris l'élaboration de spécifications de transfert pour garantir que les transferts sont effectués conformément aux spécifications avec un contrôle de qualité approprié. Les spécifications peuvent inclure la méthode de transfert, le format, la fréquence, le contenu des fichiers (noms/étiquettes/formats des variables), la modalité de transfert des tests, la détection des données identifiables, y compris la manière dont elles seront traitées et les mesures spécifiques visant à garantir la sécurité du transfert de ces données.

La classe de services Data Management peut inclure l'Ingénierie des données (traitement des données pour permettre la transmission de données de machine à machine par exemple), la Science des données (développement d'algorithmes de traitement basés sur des techniques d'Intelligence Artificielle) et l'Analyse des données (restitution des données de manière adaptée à leur interprétation et à l'aide à la prise de décision). Une CRO disposant de l'expertise appropriée peut également proposer l'Anonymisation des données à caractère personnel des sujets d'étude via des méthodes sécurisées.

Objet du traitement :	Établir et/ou suivre les règles établies pour la vérification de l'exactitude des données, la vérification, le codage des données, la saisie des données, la communication pour la prestation de services.
Finalité du traitement :	Vérification, contrôle, restauration de l'exactitude des données.
Nature du traitement :	Collecte/obtention, accès, analyse, modification, combinaison, transfert/transmission, désidentification (pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données), suppression/destruction, stockage.
Types de données à caractère personnel :	Sujets de l'étude : données sur la santé, code d'identification du sujet, données démographiques.
Durée du traitement :	Mise en place de la base de données de l'étude jusqu'au verrouillage de la base de données/transfert du fichier principal de l'étude, y compris l'anonymisation de tout ou partie des données à caractère personnel.

(10) Analyse statistique

Se réfère aux activités suivantes :

- Élaboration d'un plan d'analyse statistique (PAS) décrivant les variables à analyser et la méthode à utiliser pour effectuer l'analyse.
- Processus pour les analyses statistiques couvrant la programmation, le contrôle de la qualité et la livraison de l'analyse statistique, y compris les ensembles de données et les résultats des tableaux, figures et listings statistiques (TFLs), ainsi que le processus de communication (où, comment, accès restreint) des résultats des analyses statistiques au rédacteur médical pour l'élaboration du Rapport d'étude clinique ou à toute autre partie prenante, par exemple, le promoteur.

Objet du traitement :	Analyse des données de l'étude clinique obtenues à partir des résultats des activités de gestion des données, communication pour la prestation de services.
Finalité du traitement :	Analyses statistiques de l'étude, développement des TFLs.
Nature du traitement :	Collecte/obtention, analyse, combinaison, modification, transfert/transmission, dépersonnalisation (pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données), stockage.
Types de données à caractère personnel :	Sujets de l'étude : données de santé, code d'identification du sujet, données démographiques.
Durée du traitement :	Du développement du Plan d'analyse statistique à la fourniture du rapport d'étude clinique au promoteur.

(11) Rapport d'étude clinique (CSR)

Il s'agit de l'ensemble des activités menées pour concevoir le Rapport d'étude clinique qui rend compte avec précision des objectifs de l'étude, des méthodes, des analyses statistiques réalisées et de leurs résultats.

Les résultats sont présentés de manière agrégée, mais certaines données codées individuelles peuvent être répertoriées si nécessaire.

Objet du traitement :	Interprétation des données de l'étude clinique conformément aux résultats de l'étude, y compris les données à caractère personnel agrégées et pseudonymes.
Finalité du traitement :	Développement de la description, du résumé, de la présentation de l'analyse de la recherche via le Rapport d'étude clinique.
Nature du traitement :	Collecte/obtention, stockage, modification, transfert/transmission, effacement/destruction, désidentification (pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données).
Types de données à caractère personnel :	Sujets de l'étude : données sur la santé, code d'identification du sujet, données démographiques. Professionnels de santé : nom, fonction, lieu de travail, opinions, qualifications, expérience en recherche clinique, etc.
Durée du traitement :	Réception des résultats des analyses statistiques après l'acceptation du Rapport d'étude clinique par le promoteur.

(12) Gestion financière

Désigne l'ensemble des processus réalisés dans le cadre du suivi financier d'une Étude Clinique, et en particulier le paiement des Sites Investigateurs : honoraires et procédures complémentaires (examens supplémentaires, produits, etc.).

Objet du traitement :	Organisation du transfert de fonds, réception des confirmations de paiement.
Finalité du traitement :	Exécution des obligations financières contractuelles.
Nature du traitement :	Collecte/obtention, transfert/transmission, stockage, effacement/destruction, désidentification (pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données).
Types de données à caractère personnel :	Professionnels de santé : numéros de compte bancaire, coordonnées, localisation, fonction, etc.
Durée du traitement :	Fin de la période d'archivage pour la responsabilité financière.

(13) Information du public

La divulgation publique est le processus par lequel les résultats des analyses statistiques, la documentation élaborée pour l'étude et le Rapport d'étude clinique sont diffusés dans le domaine public de diverses manières, par exemple par les agences réglementaires qui ont mis le Rapport d'étude clinique à la disposition du public, ou par le promoteur qui a publié les informations dans des revues ou des événements scientifiques.

Objet du traitement :	Transfert des données de l'étude clinique à un tiers avec divulgation ultérieure par le tiers.
Finalité du traitement :	Divulgation obligatoire et demandée/volontaire.

Nature du traitement :	Transfert/transmission (en tant que méthodes de divulgation), dépersonnalisation (pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données), stockage, suppression/destruction.
Types de données à caractère personnel :	Personnes concernées par l'étude : données sanitaires et démographiques[25] . Professionnels de santé : nom, fonction, lieu de travail, opinions, qualifications, expérience en recherche clinique, etc.
Durée du traitement :	Réception du résultat de l'analyse statistique/CRS à la confirmation de la divulgation effectuée.

(14) Traduction des documents/données de l'étude

Désigne toutes les activités menées par la CRO pour la traduction des documents/données de l'étude, y compris les données à caractère personnel, par ex.

Objet du traitement :	Changement du code linguistique pour la représentation des données de l'étude clinique.
Finalité du traitement :	Présentation des données de l'étude clinique, y compris les données à caractère personnel, dans une langue compréhensible pour les destinataires autorisés.
Nature du traitement :	Collecte/obtention, stockage, désidentification -(pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données), traduction, suppression/destruction.
Types de données à caractère personnel :	Sujets d'étude : mêmes que (4) Collecte de données, (8) Services directs aux patients. Professionnels de santé : même chose que (3) Sélection du site et contrat.
Durée du traitement :	Fourniture du service et archivage partiel si nécessaire à des fins d'étude.

(15) Audits

Désigne toutes les activités réalisées par une CRO dans le cadre d'audits, par exemple des audits sur site, commandés lorsque l'accès à des informations confidentielles peut être exigé pour les audits où des données à caractère personnel entrant dans le champ d'application du présent Code peuvent être concernées.

Objet du traitement :	Examen des données de l'étude clinique et élaboration de preuves d'audit.
Finalité du traitement :	Vérification de la conformité légale, contractuelle, aux normes applicables/à la réglementation.
Nature du traitement :	Collecte/obtention, analyse, transfert/transmission, stockage, désidentification -(pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données), suppression/destruction.
Types de données à caractère personnel :	Toutes les données de l'étude clinique, y compris les données à caractère personnel énumérées dans toutes les catégories de services. Les données cibles dépendent de l'étendue de l'audit.

[25] Dans de rares cas, les codes d'identification des sujets peuvent être inclus dans les ensembles de données divulgués publiquement, par exemple lorsque des exigences réglementaires l'imposent. Cela n'est pas considéré comme faisant partie du cours normal des événements pour cette catégorie de service et a donc été omis. S'il est nécessaire d'inclure les codes d'identification des sujets, la CRO doit recevoir du responsable du traitement une justification et documenter cette nécessité.

Durée du traitement :	Demande d'audit et préparation jusqu'à la fin de la période d'archivage de la documentation d'audit, conformément aux exigences de la Loi applicable (droit national applicable).

(16) Fourniture de services de gestion informatique

Désigne le processus de fourniture à un client de tous les services d'administration et de gestion nécessaires pour maintenir une solution logicielle pleinement opérationnelle selon les termes du contrat de service. Le porteur du code source et du code exécutable de la solution logicielle peut être un Tiers, ainsi que le fournisseur de l'infrastructure informatique.

Les conditions de la licence d'utilisation applicables sont incluses dans le contrat de service, ainsi que toutes les conditions de livraison de la maintenance du logiciel.

Cette licence logicielle peut être achetée directement par le promoteur auprès du fournisseur informatique et utilisée par d'autres CROs conformément à leur contrat de service ou achetée par la CRO auprès du fournisseur informatique, qui doit alors figurer sur la liste des sous-traitants.

Voici quelques exemples de ces plateformes informatiques :

- Système de saisie électronique des données auquel peuvent accéder les Sites Investigateurs, le personnel chargé du contrôle et/ou de la gestion des données des CROs, ainsi que le personnel mandaté par le sponsor.
- Système de gestion des essais cliniques (CTMS).
- Une plateforme de système interactif de réponse en ligne (IWRS).
- Une plateforme de résultats électroniques rapportés par les patients (ePRO), etc.

Objet du traitement :	Mise en place d'outils/mécanismes permettant d'effectuer des flux/traitements de données programmés.
Finalité du traitement :	Maintenir l'intégrité, la disponibilité et la confidentialité des données lorsqu'elles sont traitées par la solution logicielle fournie.
Nature du traitement :	Collecte/détention, stockage, suppression/destruction.
Types de données à caractère personnel :	Sujets d'étude : les mêmes que (4) Collecte de données, (8) Services directs aux patients. Professionnels de santé : même chose que pour (3) la sélection du site et le contrat.
Durée du traitement :	Jusqu'à la fin de la consultation et de la maintenance.

(17) Mise à disposition d'une infrastructure d'hébergement physique

Désigne toutes les exigences requises pour fournir à un client les ressources physiques nécessaires à l'hébergement d'une solution logicielle, telles que les installations d'un centre de données sécurisé, y compris la capacité de traitement, l'espace de stockage des données, la connectivité internet, les systèmes de surveillance, etc. ainsi que d'éventuelles technologies de virtualisation et/ou ressources de gestion.

Ces services sont dans une large mesure "agnostiques" et l'infrastructure physique peut être mise en œuvre "dans les locaux" d'une entreprise ou d'un hôpital. Toutefois, les défis en matière de continuité de service, de sécurité et de confidentialité sont tels que la demande de fourniture d'infrastructures en tant que services ou de "services de centres de données virtualisés" augmente et que certains pays, dans les États membres de l'UE, ont désormais élaboré des normes (largement basées sur la norme ISO 27001) ou même des processus de certification pour la fourniture de ces services lorsqu'ils sont achetés pour la fourniture de solutions informatiques hébergeant des données sur la santé. Lorsque de tels services sont

fournis, ils doivent l'être avec des garanties appropriées pour protéger la confidentialité, l'intégrité et la disponibilité des données.

Pour éviter toute ambiguïté, cette classe de service est limitée à la CRO agissant en tant qu'hébergeur de données et les situations où elle sous-traite l'hébergement et la maintenance des données ne sont pas incluses dans cette classe de service.

Lorsque ce service est fourni à partir d'un pays tiers, il est important de noter que les exigences du code en matière de transferts internationaux doivent être respectées et que la localisation des installations de traitement et des administrateurs susceptibles d'accéder à distance aux données doit être dûment prise en considération.

Exemple :

Un promoteur achète à un fournisseur de technologies de l'information une solution EDC-CTMS pour gérer toutes ses études. Le contrat de service prévoit que le fournisseur informatique fournit une solution "clé en main", avec toutes les installations d'hébergement sécurisées requises (centre de données, serveurs, pare-feu, etc.).

Si le logiciel était fourni en mode "local", les installations d'hébergement sécurisé seraient celles du commanditaire et le service d'hébergement sécurisé ne serait inclus ni dans le contrat Prestataires de services, ni dans l'Accord relatif au traitement des données.

Objet du traitement :	Mise en place et maintien d'un environnement sécurisé pour l'utilisation des données.
Finalité du traitement :	Garantir des mesures techniques et organisationnelles appropriées pour l'utilisation des données.
Nature du traitement :	Collecte/détention, stockage, transfert/transmission, suppression/destruction.
Types de données à caractère personnel :	Sujets d'étude : identiques à (4) Collecte de données, (8) Services directs aux patients. Professionnels de santé : même chose que (3) Sélection du site et contrat.
Durée du traitement :	Jusqu'à la fin du service.

(18) Assistance aux utilisateurs/technique et hotline

Désigne le processus consistant à fournir un support technique aux utilisateurs d'une plateforme informatique utilisée dans le cadre d'une ou plusieurs Études cliniques. Ce type de service est généralement inclus dans le contrat de service des fournisseurs informatiques. Il peut inclure un système d'information partagé pour enregistrer et suivre chaque demande d'assistance (système de ticketing). Il exige que les données à caractère personnel des utilisateurs potentiels (investigateurs, assistants de recherche clinique, infirmières cliniques, etc.) soient collectées.

Étant donné que les utilisateurs peuvent se référer à des cas/situations pratiques, les données des Usagers de l'étude peuvent être échangées avec les hotliners. Cela peut également être le cas si la plateforme informatique comprend des systèmes ePRO ou eCOA et que l'assistance de premier niveau est assurée par le fournisseur informatique.

Objet du traitement :	Fournir une assistance technique pour résoudre les difficultés techniques liées à l'utilisation des logiciels employés pour traiter les données à caractère personnel.
Finalité du traitement :	Mesures de sécurité organisationnelles pour l'utilisation des données, garantissant l'exactitude et la disponibilité des données.
Nature du traitement :	Collecte/obtention, stockage, transfert/transmission, effacement/destruction, désidentification -(pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données).
Types de données à	Sujets d'étude : mêmes que (4) Collecte de données, (8) Services

caractère personnel :	directs aux patients. Professionnels de santé : idem (3) Sélection du site et contrat.
Durée du traitement :	Jusqu'à la fin du service.

(19) Services de démantèlement

Désigne le processus consistant à retirer/supprimer toutes les données d'un client de l'environnement informatique du fournisseur lorsque la relation contractuelle prend fin.

Le contrat de service comprend des dispositions relatives aux services de démantèlement.

Des services de mise hors service sont exigés pour toute catégorie de services prévoyant l'utilisation d'un système informatique traitant des données à caractère personnel.

L'Accord relatif au traitement des données met en œuvre les exigences correspondantes pour les données relevant du RGPD.

Exemple 1 :

Dans cet exemple, un sponsor sous-traite la réalisation d'une étude clinique à une CRO qui achète un système EDC pour cette étude. Le système EDC est un système multilocataire fourni sous la forme d'un logiciel en tant que service (SaaS).

Lorsque le contrat entre la CRO et le fournisseur informatique prend fin, les services de mise hors service consistent à supprimer toutes les données de l'étude clinique de la plateforme EDC. Dans ce cas, le logiciel EDC multilocataire reste pleinement opérationnel pour d'autres études après l'achèvement de la mise hors service.

Exemple 2 :

Dans cet exemple, un sponsor achète un système EDC-CTMS à un fournisseur de technologies de l'information pour mener une série d'études cliniques. Il est exigé que le système EDC-CTMS soit déployé dans un environnement d'hébergement dédié et sécurisé fourni par le fournisseur de technologies de l'information.

Lorsque le contrat entre la CRO et le fournisseur informatique prend fin, les services de mise hors service consistent à supprimer l'environnement d'hébergement dédié, y compris les données d'étude clinique de toutes les études qui ont été réalisées à l'aide de cette plateforme EDC-CTMS.

Objet du traitement :	Retirer les données à caractère personnel concernées de l'environnement informatique.
Finalité du traitement :	Retirer en toute sécurité toutes les données à caractère personnel de l'environnement d'hébergement.
Nature du traitement :	Suppression/destruction.
Types de données à caractère personnel :	Sujets d'étude : mêmes que (4) Collecte de données, (8) Services directs aux patients. Professionnels de santé : même chose que (3) Sélection du site et contrat.
Durée du traitement :	Jusqu'à la cessation/achèvement du service.

(20) Tenue du Trial Master File (TMF)

Le TMF est un ensemble d'enregistrements électroniques et/ou de copies papier relatifs à une étude clinique, systématisés et indexés pour en faciliter l'extraction et l'utilisation. Le service comprend

- Mise en place en accord avec les exigences du sponsor, le cas échéant,
- Attribuer des responsabilités pour le fiché (être) ;
- Identifiant les documents de l'étude qui doivent être Fichés (être) ;
- Effectuer la soumission et le traitement continus des documents,
- Stockage ;
- vérifier l'exactitude et la conformité avec les spécifications réglementaires et celles du promoteur ; et

- Transfert au sponsor.

Objet du traitement :	Collecte (de données) dans un format accessible avec un accès actif aux données.
Finalité du traitement :	Les documents essentiels de l'étude, y compris les données à caractère personnel, sont catalogués de manière standard, conformément aux BPC de l'ICH et à toutes les autres normes applicables.
Nature du traitement :	Collecte/détention, stockage, suppression/destruction.
Types de données à caractère personnel :	Sujets d'étude : toutes les données à caractère personnel pseudonymisées traitées dans le cadre de la Recherche. Professionnels de santé : toutes les données à caractère personnel traitées dans le cadre de la recherche.
Durée du traitement :	Mise en place du TMF jusqu'à la transmission du TMF à l'Organisateur.

(21) Services d'archivage

Désigne les services fournis par la CRO pour aider les Sponsors ou les Sites Investigateurs à se conformer à leurs obligations après la fin de l'étude.

Par exemple, selon les BPC et le RTC (2014/536), les promoteurs et les sites Investigateurs ont l'exigence d'archiver tous les documents liés à l'étude (TMF) et les données de l'étude clinique.

Objet du traitement :	Stockage des données dans un format accessible, aucun accès actif n'étant envisagé.
Finalité du traitement :	Maintenir la disponibilité des données pour les autorités réglementaires, les études futures, les demandes d'autorisation supplémentaires.
Nature du traitement :	Collecte/obtention, archivage, suppression/destruction, désidentification -(pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données).
Types de données à caractère personnel :	Sujets d'étude : toutes les données à caractère personnel pseudonymisées traitées dans le cadre de la Recherche. Professionnels de santé : toutes les données à caractère personnel traitées dans le cadre de la recherche.
Durée du traitement :	Pour les données pertinentes couvertes, au moins 25 ans après la fin ou l'annulation de la recherche clinique conformément au règlement sur les essais cliniques n° 536/2014 ou au règlement sur les dispositifs médicaux n° 745/2017, selon le cas ; ou toute autre durée en fonction du type d'études et selon les exigences légales/réglementaires/normatives/contractuelles applicables.

(22) Services de réglementation et de démarrage d'études

Objet du traitement :	Transfert de données à caractère personnel aux autorités réglementaires pour l'évaluation des qualifications du personnel de l'étude en tant que critère d'autorisation de la conduite de l'étude.
Finalité du traitement :	Conformité avec les obligations légales visant à garantir les qualifications appropriées des Professionnels de santé par la présentation de dossiers réglementaires attestant de la qualification adéquate des chercheurs/enquêteurs.
Nature du traitement :	Collecte/obtention, transfert/transmission, stockage, archivage, suppression/destruction.

Types de données à caractère personnel :	Professionnels de santé : nom, prénom, sexe, date de naissance, adresse postale, coordonnées électroniques et téléphoniques, coordonnées bancaires ; formation : diplôme(s) ; vie professionnelle (notamment parcours professionnel, mode et type d'exercice, éléments nécessaires à l'évaluation des connaissances dont ils disposent pour mener la recherche) ; le cas échéant, numéro d'inscription au registre partagé des professionnels de santé ; rémunération totale et rémunération perçue ; participation à d'autres études, signature.
Durée du traitement :	Comme dans (21) Services d'archivage.

(23) Organisation des réunions investigateurs

Objet du traitement :	Collecte et transfert des données à caractère personnel des Professionnels de santé aux agences de voyage, hôtels, centres de visa et autres tiers dont les services sont nécessaires pour permettre le transport des Professionnels de santé vers le lieu des réunions investigateurs.
Finalité du traitement :	Veiller à ce que l'équipe investigatrice soit bien informée du protocole de recherche et des exigences de l'étude en organisant des formations en face à face axées sur les documents de recherche, permettant aux Professionnels de santé de travailler en réseau et d'échanger leur expérience dans le cadre de recherches similaires ; cela est particulièrement important pour les recherches multinationales menées sur plusieurs sites Investigateurs.
Nature du traitement :	Collecte/obtention, transfert/transmission, stockage, désidentification -(pseudonymisation, anonymisation, agrégation, masquage, suppression d'éléments de données), suppression/destruction.
Types de données à caractère personnel :	Professionnels de santé : nom, prénom, adresse postale, coordonnées électroniques et téléphoniques, coordonnées bancaires ; fonction, pays de naissance, ville de naissance, type de carte d'identité nationale, carte d'identité nationale, statut de citoyenneté, pays de citoyenneté, nationalité, informations sur les voyages, passeport national et international, demandes de visa, informations sur les visas, dates de voyage, itinéraire, informations sur les réservations d'hôtel ; numéros de compte bancaire, etc.
Durée du traitement :	De l'acceptation par le professionnel de la santé de l'invitation à la réunion investigateurs à l'indemnisation des frais de déplacement du professionnel de la santé par la CRO ; et/ou fin de la conservation de tous les documents de responsabilité financière par la CRO.

Annexe 3 - Déclaration d'intérêts directs ou indirects

Complétez la section 5.2.5 "Conflits d'intérêts" (au niveau de l'organe de surveillance)

DÉCLARATION D'INTÉRÊTS

Je soussigné(e), ...

Reconnaître être conscient(e) de l'obligation de déclarer tous les intérêts, qu'ils soient directs ou par le biais d'un intermédiaire, avec :

1 Les CROs membres ou non-membres de l'EUCROF, telles que définis au paragraphe 1.1 "Terminologie" du Code de conduite, et dont les activités relèvent du champ d'application défini au paragraphe 1.4 "Champ d'application" du présent Code de conduite (ci-après dénommés "**CRO**") ;

2 et les entreprises, établissements ou organisations - y compris les cabinets de conseil, les cabinets d'audit et les organismes professionnels - dont les activités, les technologies et les produits relèvent de la compétence des CROs.

Je remplis cette déclaration en qualité de :

- ☐ Membre du Comité de surveillance (COSUP)
- ☐ Président du Comité de surveillance (COSUP)
- ☐ Vice-Président du Comité de surveillance (COSUP)

Je m'engage à mettre à jour ma déclaration d'intérêts dès qu'un changement survient concernant ces intérêts ou que de nouveaux intérêts apparaissent, et au moins une fois par an même s'il n'y a pas de changement.

Il vous appartient, dès réception de l'Ordre du jour d'une réunion, de vérifier si les intérêts que vous avez déclarés ou qui pourraient se manifester ponctuellement sont compatibles avec votre présence à tout ou partie de cette réunion et d'en informer la personne de contact désignée au sein du COSUP et, le cas échéant, le Président de la réunion, si possible avant la tenue de celle-ci.

En cas de conflit d'intérêts, votre présence pourrait entraîner des irrégularités dans les décisions prises ou les recommandations, références ou avis émis et entraîner la nullité de la décision prise ou de celle que le COSUP aurait pu prendre sur la base de cette délibération.

1. Votre activité principale

1.1. Occupation principale actuelle (rémunérée ou non)

Occupation professionnelle :

POSITION/ RÔLE	**NATURE DU TRAVAIL** *(Emploi/Contrat/Volontaire)*	**EMPLOYEUR / CLIENT / ORGANISATION**	**LOCATION**	**DEBUT** *(mois/année)*	**FIN** *(mois/année)*

1.2. Activités exercées à titre principal au cours des trois dernières années (rémunérées ou non)

Autres que ceux inscrits à la section 1.1

Occupation professionnelle :

POSITION/ RÔLE	**NATURE DU TRAVAIL** *(Emploi/Contrat/Volontaire)*	**EMPLOYEUR / CLIENT / ORGANISATION**	**LOCATION**	**DEBUT** *(mois/année)*	**FIN** *(mois/année)*

2. Professions secondaires

2.1 Indiquez ici vos participations actuelles ou passées à un organe décisionnel d'un organisme public ou privé dont l'activité, les technologies ou les produits relèvent de la compétence des CROs.

Il s'agit notamment des établissements de soins de santé, des formes et organismes de consultation, des organismes professionnels (sociétés savantes, réseaux de soins de santé, Caisse nationale d'assurance maladie) et des associations de patients.

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

ORGANISME *(entreprise, établissement, association)*	**POSITION** *dans l'organisation*	**RÉMUNÉRATION** *(montant à indiquer dans le tableau A1)*	**DEBUT** *(mois/année)*	**FIN** *(mois/année)*
		❑ Aucun ❑ Au déclarant ❑ A une organisation dont vous êtes membre ou employé *(veuillez préciser)*		
		❑ Aucun ❑ Au déclarant ❑ à une organisation dont vous êtes membre ou employé *(veuillez préciser)*		

2.2 Indiquez ici toutes les activités actuelles ou passées de consultant, de conseiller ou d'expert au sein d'un organisme public ou privé, dont l'activité, les technologies ou les produits relèvent de la compétence des CROs.

Sont incluses dans cette section les activités de conseil ou de représentation, la participation à un groupe de travail ou à un conseil scientifique, les activités d'audit ou la rédaction de rapports d'experts.

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

ORGANISME *(entreprise, établissement, association)*	**TÂCHES / POSTE**	**RÉMUNÉRATION** *(montant à indiquer dans le tableau A2)*	**DEBUT** *(mois/année)*	**FIN** *(mois/année)*
		❑ Aucun ❑ Au déclarant ❑ À une organisation dont vous êtes membre ou employé *(veuillez préciser)*		

		.....		
		❑ Aucun ❑ Au déclarant ❑ À une organisation dont vous êtes membre ou employé *(veuillez préciser)*		

2.3 Indiquez ici toutes les participations actuelles ou antérieures à des travaux et études scientifiques pour un organisme public ou privé, dont l'activité, les technologies ou les produits relèvent de la compétence des CROs.

La participation à des travaux scientifiques et la réalisation d'essais ou d'études cliniques ou précliniques, d'études épidémiologiques, d'études médico-économiques, d'études observationnelles, etc. doivent être mentionnées.

La fonction de membre d'un comité de surveillance et de suivi d'une étude clinique doit être déclarée dans cette section.

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

Organisme de parrainage *(entreprise, établissement, association)*	**Organisme de financement** *(si différent du parrain et si vous le connaissez)*	**Sujet** *(nom de l'étude, du produit, de la technique ou de l'indication thérapeutique)*	**REMUNERATION** *(montant à indiquer dans le tableau A.3)*	**DEBUT** *(mois/année)*	**FIN** *(mois/année)*
			❑ Aucun ❑ Au déclarant ❑ A une organisation dont vous êtes membre ou employé *(veuillez préciser)*		
			❑ Aucun ❑ Au déclarant ❑ A une organisation dont vous êtes membre ou employé *(veuillez préciser)*		

2.4 Listez ici tous les articles, discours lors de congrès, conférences, colloques, réunions publiques diverses ou formations organisés ou soutenus financièrement par des entreprises ou des organismes publics ou privés, dont l'activité, les technologies ou les produits relèvent de la compétence des CROs.

La rédaction d'articles et d'exposés doit être déclarée lorsqu'ils ont été rémunérés ou ont donné lieu à une compensation.

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

Entreprise ou organisation *(entreprise, association)*	**Pour les discours, lieu et titre de l'événement**	**Sujet** de l'article ou de l'exposé et nom du produit cible, le cas échéant	**Indemnisation des frais de voyage**	**Rémunération** *(montant à indiquer dans le tableau A.4)*	**DEBUT** *(mois/année)*	**FIN** *(mois/année)*
			❑ Oui ❑ Non	❑ Aucun ❑ Au déclarant ❑ À une organisation dont vous êtes membre ou employé *(veuillez préciser)*		
			❑ Oui ❑ Non	❑ Aucun ❑ Au déclarant ❑ À une organisation dont vous êtes membre ou employé *(veuillez préciser)*		

2.5 Indiquez ici vos activités actuelles ou passées en tant qu'inventeur et/ou propriétaire d'un brevet ou d'un produit, d'un procédé ou de toute autre forme de propriété intellectuelle non brevetée relevant de la compétence des CROs.

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

Nature de l'activité *et nom du brevet, du produit, etc.*	**Organisme** *fournissant le brevet, le produit, etc.*	**Participation aux recettes et aux bénéfices**	**Rémunération** *(montant à indiquer dans le tableau A.5)*	**DEBUT** *(mois/année)*	**FIN** *(mois/année)*
		❑ Oui ❑ Non	❑ Aucun ❑ Au déclarant ❑ A une organisation dont vous êtes membre ou employé *(veuillez préciser)*		
		❑ Oui ❑ Non	❑ Aucun ❑ Au déclarant ❑ A une organisation dont vous êtes membre ou employé *(veuillez préciser)*		

3. Activités que vous dirigez ou avez dirigées et qui ont bénéficié d'un financement de la part d'une organisation à but lucratif dont l'objet social relève de la compétence des CROs.

Le type de paiement peut prendre la forme de subventions ou de contrats d'études ou de matériel, de subventions ou de parrainage, de paiements monétaires ou en nature, d'équipements, de taxe d'apprentissage, etc.

Il s'agit des présidents, des trésoriers et des membres des bureaux et des conseils d'administration, y compris des associations et des sociétés savantes.

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

ORGANISME ET ACTIVITÉ Bénéficiaires du financement	**Organisme(s) à but lucratif (*)**	**DEBUT** *(mois/année)*	**FIN** (mois/année)

(*) Le montant payé par le(s) financeur(s) avec indication facultative du pourcentage du montant du financement par rapport au budget de l'organisme est indiqué dans le tableau B.1.

4. Participation financière au capital d'une société dont l'objet social relève de la compétence des CROs.

Les participations financières sous forme de valeurs mobilières cotées ou non cotées, qu'il s'agisse d'actions, d'obligations ou d'autres actifs financiers dans le capital d'une entreprise ou d'un secteur concerné, d'une de ses filiales ou d'une société dont elle détient une partie du capital, dans la mesure de votre connaissance immédiate et attendue, doivent être déclarées.

Il est exigé que vous indiquiez le nom de l'établissement, de l'entreprise ou de l'organisation, le type de participations financières et leur montant en valeur absolue et en pourcentage du capital détenu.

(Les fonds d'investissement de type "open-end trust" ou "unit trust" dans des produits collectifs - dont la personne ne contrôle ni la gestion ni la composition - sont exclus de la déclaration).

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

ORGANISME	**TYPE D'INVESTISSEMENT (*)**

(*) Le pourcentage de l'investissement dans le capital de l'organisme et le montant détenu sont indiqués dans le tableau C.1.

5. Les parents proches ayant des activités ou des intérêts financiers dans tout organisme dont l'objet social relève de la compétence des CROs.

Les personnes concernées sont :
- *votre partenaire (conjoint, concubin ou partenaire civil), ainsi que les parents (père et mère) et le(s) enfant(s) de ce dernier ;*
- *vos enfants ;*
- *vos parents (père et mère).*

Dans cette section, vous devez déclarer si vous êtes au courant :
- *des professions (au sens des sections 1 à 3 du présent document) exercées ou dirigées ou exercées au cours des 3 dernières années par vos proches parents*
- *de toute participation financière directe dans le capital d'une société (au sens de la section 4 du présent document) au-delà d'un montant de 5 000 euros ou de 5 % du capital détenu par vos proches.*

Vous devez identifier le Tiers concerné uniquement par votre lien de parenté.

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

Parent(s) proche(s) ayant un lien avec les organisations suivantes *(La relation est indiquée dans le tableau D.1.)*	**ORGANISMES CONCERNÉS**	**Professions (actuelles ou au cours des 5 dernières années)**	**Participation au capital** *Participation financière directe actuelle supérieure à un montant de 5 000 euros ou à 5 % du capital (Le montant est indiqué dans le tableau)*

Parent(s) proche(s) ayant un lien avec les organisations suivantes *(La relation est indiquée dans le tableau D.1.)*	**ORGANISMES CONCERNÉS**	**Professions (actuelles ou au cours des 5 dernières années)**	**Participation au capital** *Participation financière directe actuelle supérieure à un montant de 5 000 euros ou à 5 % du capital (Le montant est indiqué dans le tableau)*

6. Autres intérêts que vous pensez devoir porter à l'attention du COSUP

- ❑ Je n'ai aucun intérêt à déclarer dans cette section.
- ❑ Actuellement ou au cours des trois dernières années :

ÉLÉMENT OU FAIT PERTINENT	**COMMENTAIRES** *(le montant des sommes perçues est indiqué dans le tableau E.1.)*	**Début de l'année**	**Fin de l'année**

7. Si vous n'avez inscrit aucune information après le point 1, cochez la case et signez la dernière page. ❑

[A REMPLIR le cas échéant : vous pouvez être sanctionné pour avoir sciemment omis de remplir ou de modifier une déclaration d'intérêts afin d'en actualiser les données ou pour avoir fourni des informations trompeuses qui portent atteinte à l'honnêteté de cette déclaration].

8. Tableaux des mentions à ne pas divulguer

Tableau A.1

ORGANISME	**MONTANT REÇU**

Tableau A.2

ORGANISME	**MONTANT REÇU**

Tableau A.3

ORGANISME	**MONTANT REÇU**

Tableau A.4

ENTREPRISE ou ORGANISME	**MONTANT REÇU**

Tableau A.5

ORGANISME	**MONTANT REÇU**

Tableau B.1

ORGANISME	**Pourcentage du montant reçu** du financement par rapport au budget de fonctionnement de l'organisme et au montant versé par le financeur

Tableau C.1

ORGANISME	**Pourcentage** *de l'investissement dans le capital de l'organisme et du montant détenu*

Tableau D.1

	SALARIÉ	**ACTIONNAIRE**			
ORGANISME	**Poste de travail** *(Préciser, le cas échéant, s'il s'agit d'un poste à responsabilités)*	**Montant** *Si ≥ 5 000 EUR ou 5 % du capital*	**Relation**	**Démarrage** *(mois/année)*	**Fin** *(mois/année)*

Tableau E.1

ÉLÉMENT OU FAIT PERTINENT	**PRÉCISEZ les montants reçus, le cas échéant**

Fait en

sur

Signature (obligatoire)
(Données à ne pas divulguer)

EUCROF est le responsable du traitement dans le but de prévenir les conflits d'intérêts en prenant en considération les intérêts ainsi déclarés dans les ordres du jour des réunions tenues par le COSUP, conformément aux exigences du Code de conduite approuvé par les autorités compétentes en matière de protection des données à caractère personnel. Les informations recueillies dans ce formulaire seront sauvegardées et publiées sur le site internet de l'EUCROF à des fins de transparence, à l'exception des informations figurant dans la partie 8.

Ces informations seront conservées pendant [À COMPLÉTER] ans à compter de leur transmission à l'EUCROF.

Conformément à la Loi relative à l'informatique et aux libertés et à l'Acte réglementaire européen sur la protection des données, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant le responsable de la protection des données de l'EUCROF à l'adresse suivante [À COMPLÉTER]. Vous disposez également d'un droit à l'effacement et à la limitation de vos données, ainsi que du droit d'introduire une réclamation auprès de la CNIL.

Vous pouvez également définir des directives relatives au sort de vos données à caractère personnel après votre décès en vous adressant directement au responsable de la protection des données de l'EUCROF pour obtenir des instructions spécifiques, ou à tout tiers de confiance numérique labellisé par la CNIL et inscrit sur le registre unique dont les modalités et l'accès seront fixés par décret en Conseil d'État pour les directives générales.

Les coordonnées du Délégué à la Protection des Données de l'EUCROF sont les suivantes : [À COMPLÉTER]

Annexe 4 - Engagement d'indépendance et de confidentialité

Complétez la section 5.2.5 "Conflits d'intérêts" (au niveau de l'organe de surveillance)

ANNEXE 5

MODÈLE D'ENGAGEMENT ET DE CONFIDENTIALITÉ

Je soussigné€, ...

prendre les engagements d'indépendance et de confidentialité suivants dans le cadre de ma nomination à mon poste :

- ☐ Membre du Comité de surveillance (COSUP)
- ☐ Président du Comité de surveillance (COSUP)
- ☐ Vice-Président du Comité de surveillance (COSUP)

Indépendance

Je m'engage à exercer mon mandat au sein du COSUP en toute indépendance et à ne pas me soumettre à des pressions qui pourraient influencer mon comportement dans l'exercice de mon mandat.

En particulier, je m'engage à vérifier systématiquement avant chaque réunion si les intérêts que j'ai déclarés (voir annexe 4 du Code de conduite) ou qui pourraient survenir de manière ponctuelle sont compatibles avec ma présence pendant tout ou partie de ladite réunion.

À défaut, je m'engage à en avertir la personne de contact désignée au sein du COSUP et, le cas échéant, le Président de la réunion, si possible avant sa tenue.

Je m'engage à me retirer de la réunion en cas de conflit d'intérêts, ma présence pouvant entraîner des irrégularités dans les décisions prises ou les recommandations, références ou avis émis et entraîner la nullité de la décision prise ou de celle que le COSUP aurait pu prendre sur la base de ladite Délibération.

Confidentialité

Je reconnais que tous les faits, actes et informations auxquels j'ai accès directement ou indirectement dans l'exercice de mon mandat, y compris non seulement ce qui m'a été dit, mais aussi ce que j'ai vu, entendu ou compris, sont des informations confidentielles ("**Informations confidentielles**").

L'obligation de confidentialité à laquelle je suis tenu consiste à ne pas divulguer, par quelque moyen que ce soit, les Informations Confidentielles dont j'ai eu connaissance dans l'exercice de mon mandat tant aux membres de l'EUCROF - sauf s'ils sont eux-mêmes autorisés à connaître les Informations Confidentielles en question - qu'à des personnes extérieures.

Le fait que d'autres personnes aient connaissance des informations confidentielles n'affecte pas leur caractère confidentiel et secret.

Cette obligation de confidentialité reste contraignante après la fin de mon mandat, quelle que soit sa durée.

Fait dans ..... Signature

Fin du document