# Directives étendues version 2.0

## Exigences de la certification CoreTrustSeal en matière de dépôts de données fiables : Directives étendues 2020 à 2022

Le présent document est une traduction française non-officielle de « CoreTrustSeal Trustworthy Data Repositories Requirements: Extended Guidance 2020–2022 » Version v02.00-2020-2022, publié le 20 novembre, 2019 et accessible sur le site de CoreTrustSeal (https://www.coretrustseal.org/why-certification/requirements/) et sur Zenodo (10.5281/zenodo.3632533)

CoreTrustSeal est un organisme communautaire sans but lucratif que promeut le développement d'infrastructures de données durables et fiables. « CoreTrustSeal Extended Guidance » a été conçu pour faciliter le travail des évaluateurs de demandes de certification CoreTrustSeal (CTS) mais également pour fournir des informations et conseils aux entrepôts de données désireux d'entreprendre une démarche de certification CTS.

La présente traduction a été produite par le Réseau Portage, avec le soutien de l'Association des bibliothèques de recherche du Canada et de la Nouvelle organisation de l'infrastructure de recherche numérique (NOIRN) du Canada. Cette traduction ne se substitue pas au document original en langue anglaise qui seul fait autorité dans le processus de certification CTS.

Pour plus d'informations sur CoreTrustSeal et le processus de certification CTS voir le site https://www.coretrustseal.org/.

Pour plus d'informations sur le Réseau Portage, voir le site https://portagenetwork.ca/fr/. Pour plus d'informations sur la NOIRN, voir https://engagedri.ca/fr/.

# Table des matières

# Introduction

Ce document contient le texte intégral du document ***CoreTrustSeal Trustworthy Data Repositories Requirements*** *for 2020–2022* avec des paragraphes d'introduction sur le contexte et les directives générales.

En plus des exigences de la certification CoreTrustSeal, qui demeurent inchangées pour la période 2020 à 2022, ce document présente des **directives étendues** pour les évaluateurs et les demandeurs de la certification CoreTrustSeal. Le texte des Directives étendues peut être actualisé au cours de la période 2020 à 2022 sous réserve de l'approbation du conseil de la certification CoreTrustSeal. Ce document contient aussi une référence au glossaire terminologique.

Le présent document a été conçu pour maximiser l'uniformité des évaluations compte tenu de la grande diversité des demandeurs de certification CoreTrustSeal ; il s'adresse principalement aux évaluateurs, mais il peut être utile aux demandeurs lorsque ceux-ci préparent l'autoévaluation liée à leur demande.

# Contexte et directives générales

Les exigences de la certification CoreTrustSeal pour les dépôts de données fiables (*CoreTrustSeal Trustworthy Data Repositories Requirements)* décrivent les caractéristiques générales des dépôts fiables. Toutes les exigences sont obligatoires et elles sont évaluées indépendamment l'une de l'autre. Bien que certains chevauchements soient inévitables, la duplication des preuves demandées pour chaque exigence a été réduite au minimum. Les options des listes de contrôle (par exemple, type de dépôt et niveau de curation) ne sont pas exhaustives et pourront être peaufinées à l'avenir. On encourage les demandeurs à ajouter d'autres options.

Chaque exigence est accompagnée d'un texte explicatif décrivant les informations et les preuves que les demandeurs doivent fournir pour permettre une évaluation objective.

Les demandeurs doivent indiquer le degré de conformité pour chaque exigence :

0 – Sans objet
1 – Le dépôt n'a pas encore considéré l'exigence.
2 – Le dépôt a un concept théorique pour l'exigence.
3 – Le dépôt est en phase d'application de l'exigence.
4 – Le dépôt applique l'exigence intégralement.

Les degrés de conformité sont des indicateurs de la progression autoévaluée par les demandeurs ; or, les évaluateurs jugent la conformité en fonction des déclarations et des preuves à l'appui. Si des demandeurs estiment qu'une exigence est sans objet (0), ceux-ci doivent justifier leur réponse avec des précisions. Les degrés de conformité 1 et 2 ne sont pas suffisants pour l'acceptation des demandes. La certification peut être accordée si certaines exigences sont en phase d'application (3).

Les déclarations fournies par les demandeurs doivent inclure des liens vers les preuves accessibles en ligne. Étant donné que le processus de certification de base ne comprend pas de visite sur place de la part des auditeurs, ces preuves accessibles au public fournissent une assurance transparente de bonne pratique. Les liens URL doivent être vérifiés juste avant de soumettre les demandes.

Toutes les réponses doivent être rédigées en anglais. Bien que nous nous efforcions de jumeler les évaluateurs et les demandeurs selon la langue et la discipline, le jumelage conséquent n'est pas toujours possible. La traduction intégrale des preuves n'est pas obligatoire, mais si des preuves en langue autre que l'anglais sont fournies, un résumé en anglais doit être inclus dans la déclaration.

Aucune divulgation d'informations sensibles n'est obligatoire pour obtenir la certification CoreTrustSeal, mais des dispositions sont prévues dans le processus de certification pour les

dépôts qui souhaitent partager des éléments de preuve contenant des informations confidentielles.

La certification CoreTrustSeal est valable pendant trois ans à compter de la date d'attribution. Bien que les systèmes et les capacités des dépôts évoluent constamment en fonction de la technologie et des besoins des utilisateurs, il est possible qu'ils ne subissent pas de changements majeurs dans ce laps de temps. Les organisations dont les processus opérationnels et les documents sont bien gérés devraient être en mesure de présenter une nouvelle demande avec des révisions minimes après trois ans, sauf si :

- Les organisations, leur collecte de données ou leur communauté désignée changent de manière considérable ;
- La mise à jour des exigences de CoreTrustSeal a eu un impact sur les demandeurs.

Les exigences de CoreTrustSeal font l'objet d'un examen et d'une révision tous les trois ans. Celles-ci ne touchent pas les demandeurs qui ont été retenus jusqu'à ce qu'ils demandent un renouvellement.

## Glossaire terminologique

Veuillez consulter le glossaire des exigences de la certification CoreTrustSeal en matière de dépôts fiables : https://doi.org/10.5281/zenodo.3632563.

## Directives générales étendues

### Introduction : points généraux

La révision des informations probantes tous les trois ans à des fins de certification uniquement n'est pas efficace. La gestion continue des informations nécessaires au fonctionnement des services d'un dépôt devrait être suffisante pour demander et maintenir la certification. Les dépôts qui documentent suffisamment leurs politiques et procédures pour garantir une qualité constante, atténuer le risque de départ du personnel, etc. devraient uniquement préparer les réponses aux demandes et gérer les versions publiques de leurs preuves.

Les évaluateurs peuvent proposer un degré de conformité différent de celui choisi par les demandeurs. Si les évaluateurs établissent un degré de conformité inférieur, ils en expliqueront la raison. Si le degré de conformité est inférieur à 4, on s'attend à une progression de la conformité à l'exigence lors du renouvellement de la certification.

Il est impossible de couvrir tous les scénarios de dépôt possibles dans les directives ou les directives étendues. De même, tous les points de toutes les exigences ne sont pas obligatoires. Les réponses des demandeurs doivent faire référence aux questions dans le texte du guide et fournir des réponses basées sur leur contexte local. L'évaluation finale d'une exigence dépend de l'exhaustivité et de la qualité de la réponse. Les évaluateurs recherchent des déclarations claires et ouvertes quant aux preuves particulières des demandeurs.

Les concepts et la terminologie utilisés dans les exigences sont inspirés du modèle de référence du Open Archival Information System ou OAIS (Système ouvert d'archivage d'information). L'utilisation de la terminologie du OAIS peut contribuer à assurer la compréhensibilité et la clarté de la demande ; on encourage donc fortement les demandeurs à se familiariser avec le OAIS avant de préparer leurs réponses aux exigences. Le rapport de 2014 intitulé *DPC Technology Watch Report « Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition) »* de Brian Lavoie (https://doi.org/10.7207/twr14-02) fournit une introduction utile au modèle de référence OAIS.

## Information/preuve manquante

Le processus de certification CoreTrustSeal repose sur des réponses étayées par des preuves. La qualité des preuves publiques à l'appui devrait s'améliorer au fil du temps. Les demandes sont plus difficiles à évaluer si les informations sont manquantes, insuffisantes ou ambiguës, si les liens URL sont rompus ou si les déclarations probantes se font des renvois les unes aux autres.

La familiarité ou la connaissance approfondie du dépôt par l'évaluateur doit être exclue de l'évaluation des preuves disponibles. La déclaration finale et publique des preuves doit également être claire pour que les dépôts des pairs puissent la comprendre.

Les évaluateurs ne chercheront probablement pas de preuves sur les sites web des demandeurs. Si les informations fournies ne suffisent pas à la prise de décision, les demandes seront renvoyées avec une explication des raisons pour lesquelles les preuves sont insuffisantes. Dans ce cas, les évaluateurs ne fourniront pas de degré de conformité.

## Compréhensibilité de la documentation

Les évaluateurs et les lecteurs de l'évaluation finale et publique doivent être en mesure de comprendre les réponses aux exigences sans avoir à lire en détail les preuves à l'appui. Lorsque des documents plus longs sont présentés comme preuves, ou qu'un document est utilisé comme preuve pour plus d'une exigence, les demandeurs doivent faire référence aux sections pertinentes avec précision et citer ou résumer l'information dans leur réponse.

## Documentation en langue autre que l'anglais

Les documents rédigés en langue autre que l'anglais sont acceptables si leur contenu est suffisamment et clairement expliqué dans un résumé en anglais. Ce résumé peut être assez bref pour certains types de documents (par exemple, une liste de formats préférés), mais doit être plus long pour d'autres (par exemple, un document sur la politique de préservation).

## Documentation sensible et autre documentation interne

La certification CoreTrustSeal n'exige pas que les informations justificatives confidentielles, protégées commercialement ou présentant un risque pour la sécurité soient divulguées publiquement. Cette exemption s'applique également aux documents qui sont seulement disponibles sur l'intranet d'un dépôt. Les demandeurs peuvent avoir des informations commerciales comportant des informations sensibles et des preuves pertinentes pour la certification CoreTrustSeal. Ces preuves peuvent être soumises de manière confidentielle aux évaluateurs et aux documents nommés et décrits dans la demande[1]. Avec le temps, les demandeurs devraient séparer les preuves pertinentes des documents confidentiels et s'assurer qu'une version publique est disponible pour la prochaine révision.

Si la documentation n'existe pas encore, est en cours de réalisation ou est actuellement réservée à un usage interne (par exemple, un wiki), une date de disponibilité publique doit être indiquée dans la demande. La certification peut être approuvée selon ces assurances. Les demandeurs doivent fournir la documentation publique lors du renouvellement de leur certification.

## Structure et longueur des demandes

Les demandes en cours sont uniquement divulguées aux évaluateurs et au conseil de CoreTrustSeal, mais les demandes retenues sont rendues publiques. Les demandeurs doivent donc tenir compte de tous ces publics. Les demandes ne doivent pas être présentées sous forme de questions-réponses pour chaque point des directives. Les demandes doivent comporter des réponses détaillées pour chaque exigence en intégrant les éléments pertinents des directives et des directives étendues fournies.

Le conseil de CoreTrustSeal reconnait que les demandeurs proviennent de diverses organisations dont la mission, la taille et la complexité varient tant sur le plan de la structure organisationnelle que de la variété des données collectées. Même les directives étendues ne peuvent pas couvrir tous les sujets et types de preuves qui pourraient être pertinents pour la demande. Nous comprenons également que les explications sur la pertinence des preuves fournies nécessitent de l'espace, surtout si elles ne sont pas disponibles en anglais. Le conseil n'impose pas de longueur minimale ou maximale pour les réponses, mais d'après les demandes antérieures, même les déclarations les plus complexes se situent généralement autour de 500 mots et excèdent rarement 800 mots. Si possible, les déclarations probantes doivent être étayées par des liens publics vers la documentation régissant votre organisation et vos objets numériques. Ces preuves publiques offrent la meilleure garantie qu'une organisation gère ses collections comme un dépôt de données fiable.

Les demandeurs ne doivent pas avoir à répéter de longues portions de texte dans les différentes réponses aux exigences. Dans les cas où les preuves s'appliquent à plus d'une exigence, un résumé des informations pertinentes doit être ajouté avec un renvoi à la réponse appropriée pour plus de détails.

[1] Les documents confidentiels devraient être transmis au secrétariat de CoreTrustSeal à info@coretrustseal.org

# Exigences

## Information contextuelle

**R0. Veuillez préciser le contexte de votre dépôt.**

**– Type de dépôt. Choisissez tous les types pertinents dans la liste suivante :**

- **Dépôt spécialisé par domaine ou sujet**
- **Dépôt institutionnel**
- **Système de dépôt national, y compris gouvernemental**
- **Dépôt de publication**
- **Bibliothèque**
- **Musée**
- **Archive**
- **Dépôt pour projet de recherche**
- **Autre (veuillez préciser)**

***– Brève description du dépôt***

***– Brève description de la communauté désignée***

***– Niveau de curation effectuée. Choisissez tous les niveaux pertinents dans la liste suivante :***

A. **Contenu distribué tel que déposé**
B. **Curation de base – p. ex., vérification sommaire, ajout de métadonnées ou de documentation de base**
C. **Curation accrue – p. ex., conversion des formats, amélioration de la documentation**
D. **Curation sur le plan des données – comme dans la réponse C, avec de l'édition supplémentaire des données déposées pour la précision**

**Commentaires**

***– Partenaires internes/externes. Veuillez les énumérer le cas échéant.***

***– Résumé des changements importants depuis la dernière demande (le cas échéant).***

***– Autre information pertinente.***

**Réponse**

### Directives :

Les informations suivantes fournissent le contexte dont les évaluateurs ont besoin pour évaluer pleinement les réponses aux autres exigences. Les demandeurs doivent donc impérativement fournir des réponses détaillées à chaque question pour l'ensemble de la demande. Veuillez choisir parmi les options suivantes et fournir des détails pour les éléments qui apparaissent dans l'exigence liée au contexte.

***(1) Type de dépôt***. Cet élément aidera les évaluateurs à comprendre quelle fonction remplit votre dépôt. Choisissez le type qui correspond le mieux à votre dépôt (choisissez tous les types pertinents). Si aucun type n'est approprié, n'hésitez pas à fournir un autre type descriptif. Vous pouvez également fournir d'autres détails pour aider l'évaluateur à comprendre votre type de dépôt.

***(2) Brève description du dépôt***. Présentez brièvement le dépôt ; ajoutez surtout des informations sur le type de données acceptées par le dépôt (c.-à-d. la portée de sa collection). Si le dépôt a des partenaires externes ou s'il fait partie d'un réseau ou d'une organisation apparentée, la réponse devrait idéalement inclure un organigramme et une description de la structure organisationnelle globale.

***(3) Communauté désignée***. Une définition claire de la communauté désignée démontre que les demandeurs comprennent la portée, la base de connaissances et les méthodologies — y compris les logiciels et les formats préférés — de la communauté ou des communautés d'utilisateurs qu'ils ciblent. Précisez suffisamment votre réponse de sorte que les évaluateurs puissent évaluer la pertinence des mesures de curation et de préservation décrites dans la demande.

***(4) Niveau de curation***. Ce point sert à déterminer si le dépôt distribue son contenu aux consommateurs de données sans modification ou si le dépôt ajoute de la valeur en améliorant le contenu d'une manière quelconque. Tous les niveaux de curation supposent (1) que les dépôts initiaux sont sauvegardés tels quels et que les modifications ne sont effectuées que sur des copies de ces originaux, et (2) que les métadonnées qui permettent à la communauté désignée de comprendre et d'utiliser les données de manière indépendante (c'est-à-dire sans avoir à consulter le créateur original) sont présentes lors du versement ou ajoutées par le dépôt. Les annotations ou les modifications doivent être conformes aux modalités de la licence convenue avec le producteur de données et relever clairement des compétences des personnes chargées de la curation. Ainsi, le dépôt devra démontrer que de telles annotations ou modifications sont effectuées et documentées par des experts appropriés et que l'intégrité de toutes les copies originales est maintenue. Avec cette information, les évaluateurs pourront mieux évaluer les autres exigences de certification. Vous pouvez ajouter d'autres détails qui aideront à comprendre les niveaux de curation que vous pratiquez.

***(5)Partenaires internes/externes***. Veuillez fournir une liste des partenaires avec lesquels votre organisation travaille, en décrivant la nature de la relation (organisationnelle, contractuelle, etc.) et en indiquant si le partenaire a procédé à une évaluation du dépôt fiable. Si une fonction ou un élément probant ne relève pas directement des demandeurs, cette fonction ou cet élément probant s'inscrit dans cette catégorie. Il peut s'agir d'une organisation hôte ou d'une autre relation d'approvisionnement interne, d'une impartition ou d'un autre recours externe. Ces relations peuvent inclure, notamment : les services fournis par votre établissement, le stockage fourni par autrui dans le cadre d'une redondance à copies multiples ou l'adhésion à des organisations susceptibles d'assurer la gestion de votre collection de données en cas de problème de continuité des activités. De plus, veuillez énumérer les exigences de certification pour lesquelles le partenaire fournit la fonctionnalité ou le service concerné en totalité ou en partie, y compris les contrats ou les ententes de niveau de service en vigueur. Puisque l'impartition sera presque toujours partielle, vous devrez quand même fournir des preuves appropriées pour les exigences de certification qui ne sont pas imparties et pour les parties du cycle de vie des données que vous contrôlez. Il est préférable que les partenaires d'impartition possèdent des qualifications/certifications, notamment la certification CoreTrustSeal (et ses prédécesseurs). Toutefois, il n'est pas nécessaire qu'ils soient certifiés. Nous comprenons que ce domaine peut être complexe à définir et à décrire, mais ces détails sont essentiels pour garantir un processus d'évaluation complet.

***(6) Résumé des changements importants depuis la dernière demande.*** La certification CoreTrustSeal est assortie d'une attente d'amélioration continue. Les dépôts en cours de renouvellement de certification doivent indiquer brièvement aux évaluateurs tous les changements importants survenus dans les systèmes techniques, la communauté désignée, le financement, etc. au cours des trois années précédentes. Dans ce contexte, veuillez consulter les commentaires formulés par les évaluateurs de votre précédente demande de certification CoreTrustSeal. Vous devez ajouter des informations détaillées sur un changement à l'exigence appropriée.

***(7) Autre information pertinente***. Les responsables du dépôt peuvent souhaiter ajouter des informations contextuelles supplémentaires qui ne sont pas couvertes par les exigences, mais qui peuvent être utiles aux évaluateurs. Par exemple, vous pouvez décrire :

- L'utilisation et l'effet des fonds de données du dépôt (citations, utilisation dans d'autres projets, etc.) ;
- Le rôle que joue le dépôt sur le plan régional, national ou mondial ;
- Les regroupements ou réseaux d'organismes mondiaux auxquels le dépôt appartient.

## Directives étendues R0

### Type de dépôt et brève description du dépôt

Si vous choisissez plus d'un type pour désigner votre dépôt, veuillez expliquer dans la section *Brève description du dépôt* la manière dont ces différents rôles sont assumés. Cette explication peut faire référence à des collections, des types et des formats de données ainsi que les disciplines que le dépôt prend en charge.

### Brève description de la communauté désignée

Comme la définition l'indique (voir le glossaire), un dépôt peut avoir une communauté désignée composée de différentes « sous-communautés », pour différentes collections par exemple. Le cas échéant, les demandeurs doivent fournir une définition et une description suffisamment détaillée de chacune de ces sous-communautés. De plus, la communauté désignée peut être plus petite que l'ensemble des utilisateurs d'un dépôt. Les collections numériques d'un musée d'histoire naturelle peuvent intéresser un large groupe d'utilisateurs intéressés, y compris le grand public. Néanmoins, le musée peut définir sa communauté désignée de manière plus restreinte (p. ex. biologistes et anthropologues effectuant des recherches en histoire naturelle).

Pour bien servir leur communauté désignée, les responsables des dépôts doivent avoir une connaissance approfondie de la composition, des compétences, de la base de connaissances et des besoins de la communauté désignée et de la façon dont ces éléments peuvent évoluer au fil du temps. Pour l'ensemble de la demande, les preuves doivent démontrer une compréhension des exigences de curation (contexte supplémentaire, formats préférés, etc.) pour servir la communauté désignée de manière optimale (y compris les sous-communautés, le cas échéant) et prouver que les demandeurs surveillent et réagissent à l'évolution des besoins de la communauté désignée.

Un dépôt ayant une communauté désignée très précise et restreinte pourrait facilement indiquer la base de connaissances attendue (p. ex., le degré de compréhension de la génétique ou le niveau d'expertise dans l'utilisation d'un logiciel statistique). En revanche, une communauté désignée large (c'est-à-dire composée de plusieurs communautés d'utilisateurs) nécessite que les responsables des dépôts aient une compréhension suffisante de toutes ses bases de connaissances et offrent une multitude de documents contextuels pour s'assurer que tous les membres de la communauté désignée comprennent ses données. En ce qui concerne la définition de la base de connaissances de la communauté désignée, les demandeurs doivent indiquer explicitement toutes leurs suppositions tacites, telles que les compétences langagières (étrangères), l'accès à des systèmes d'exploitation ou à des navigateurs Internet particuliers, l'utilisation de certains logiciels, etc.

### Niveau de curation effectuée

Plus d'une option (A, B, C ou D) du niveau (ou de l'étendue) de curation peut être sélectionnée, selon le type de données et les modalités de curation convenues avec le déposant. Lorsque les dépôts pratiquent la curation à plus d'un niveau, les demandeurs doivent ajouter des informations supplémentaires sur la proportion des données de la collection traitée à ces niveaux respectifs de curation. Les réponses aux exigences doivent ensuite traiter de la façon dont les flux de travail de curation reflètent les différents niveaux de curation, et de la façon dont les niveaux de curation se rapportent au niveau de préservation. Par exemple, est-ce que les objectifs et les actions de préservation sont les mêmes pour toutes les données, quel que soit le niveau de curation ?

En plus d'indiquer les niveaux de curation, les responsables des dépôts doivent ainsi prouver qu'ils assurent l'accessibilité à long terme des données en fonction de l'évolution des besoins de la communauté désignée. Cela pourrait être plus difficile au niveau de curation A et B, car sans normalisation des formats de fichiers soumis à un format de préservation commun, des migrations de format à l'avenir pourraient être difficiles en raison de l'hétérogénéité de la collection. De même, l'absence de métadonnées et de documentation étoffées peut constituer un risque pour l'utilisation continue des données.

Les évaluateurs s'attendront à une augmentation de la rigueur quant à la provenance formelle, l'intégrité et la gestion des versions (journaux des modifications, etc.) à mesure que les niveaux de curation progressent de A à D.

### Partenaires internes/externes

Si les dépôts ont plus d'un partenaire, un organigramme pour illustrer le processus de collaboration interne ou d'impartition pourrait aider les évaluateurs. Le fait d'avoir plusieurs partenaires internes/externes (p. ex., un pour le stockage, un pour la gestion des sites web) est acceptable à condition que toutes les relations soient clairement indiquées. Les évaluateurs s'attendront à ce que les demandeurs révisent leur réponse dans cette section si leurs déclarations de preuve, plus loin dans la demande, font référence à des entités qui ne sont pas mentionnées ici.

.

**Autres informations pertinentes**

Les responsables des dépôts peuvent évoquer ici leur fiche de re3data (http://www.re3data.org/), le nombre d'employés, la taille de la collection, le nombre moyen de téléchargements, leur évolution dans le temps, leur modèle commercial ou leur modèle de financement, etc. Une description claire et cohérente de l'approche organisationnelle dans son ensemble est généralement utile.

# Infrastructure organisationnelle

## 1. Mission/portée

**R1. Le dépôt a pour mission explicite de fournir l'accès aux données de son domaine et de les préserver.**

Degré de conformité :

**Réponse**

### Directives :

Les dépôts ont la responsabilité de gérer les objets numériques et de s'assurer que les matériaux sont conservés dans l'environnement approprié pendant des périodes appropriées. Les déposants et les utilisateurs doivent être conscients que la préservation et l'accès continu aux données constituent des rôles explicites des dépôts.

Pour cette exigence, veuillez décrire :

- La mission de votre organisation en matière de préservation des données et d'accès à celles-ci, et ajoutez les liens vers des déclarations explicites de cette mission.
- Le degré d'approbation que la mission a reçu au sein de l'organisation.

La preuve de conformité à cette exigence peut prendre la forme d'un énoncé de mission public approuvé, de rôles imposés par les bailleurs de fonds, d'un énoncé de politique signé par le conseil d'administration.

### Directives étendues R1.

Si la préservation des données n'est pas mentionnée dans la mission du dépôt, cette exigence ne peut pas avoir un degré de conformité de 3 ou plus.

## 2. Licences

**R2. Le dépôt maintient toutes les licences en vigueur couvrant l'accès aux données et l'utilisation de celles-ci et vérifie le respect des licences.**

Degré de conformité :

**Réponse**

### Directives :

Les dépôts de données doivent disposer d'un modèle de droits approprié couvrant l'accès aux données et l'utilisation de celles-ci, communiquer au sujet des droits avec les utilisateurs et surveiller le respect des droits. Cette exigence concerne les règles d'accès et les licences établies par le dépôt de données lui-même, ainsi que les codes de conduite généralement acceptés dans le secteur concerné pour l'échange et le bon usage des connaissances et des informations. Les preuves doivent démontrer que le dépôt a mis en place des contrôles suffisants en fonction des critères d'accès de ses fonds de données, ainsi que des preuves que toutes les licences et tous les processus pertinents sont bien gérés.

Pour cette exigence, veuillez décrire :

- Les ententes de licence en usage ;
- Les conditions d'utilisation (droits de propriété intellectuelle, distribution, utilisation prévue, protection des données sensibles, etc.) ;
- La documentation sur les mesures en cas de non-respect des conditions d'accès et d'utilisation.

Notez que si tous les fonds de données sont entièrement publics et exempts de conditions imposées aux utilisateurs — telles que des exigences d'attribution ou une entente pour rendre l'analyse secondaire librement accessible — il suffit de l'affirmer.

Les dispositions relatives à l'éthique et à confidentialité qui ont un impact sur les licences sont traitées dans le document R4 (Confidentialité/éthique). L'assurance que les licences de dépôt fournissent des droits suffisants pour que le dépôt puisse maintenir, préserver et offrir l'accès aux données doit être abordée dans la section R10 (Plan de préservation).

### Directives étendues R2.

Les stipulations relatives à l'accès aux données et à leur utilisation pourraient être définies dans un ensemble de conditions générales standard ou différenciées en fonction du déposant ou du jeu de données. Pour les données sensibles, en particulier, les licences peuvent préciser les limites d'utilisation, l'environnement d'utilisation (salle sécurisée, accès à distance sécurisé) et les types d'utilisateurs (chercheur autorisé, chercheur formé, etc.). Les options de licence les plus courantes comprennent, notamment, celles proposées par Creative Commons (https://creativecommons.org/) telles que les licences CC 0 Waiver (Renonciation) et Public Domain Data (données du domaine public).

Bien qu'il puisse être difficile de recenser les cas de non-conformité, il faut prévoir des conséquences en cas de découverte de non-conformité (p. ex. des sanctions quant à l'accès/utilisation actuelle ou future des données). Dans le cas de la divulgation de données personnelles sensibles, il peut y avoir de lourdes sanctions juridiques ayant un effet à la fois sur l'utilisateur et sur le dépôt. Idéalement, les dépôts devraient avoir une politique publique en cas de non-conformité.

Un degré de conformité 4 est nécessaire si les demandeurs donnent actuellement accès à des données personnelles.

## 3. Continuité d'accès

**R3. Le dépôt dispose d'un plan de continuité pour assurer l'accès permanent et la préservation de ses fonds.**

Degré de conformité :

**Réponse**

### Directives :

Cette exigence couvre la gouvernance liée à l'exploitation continue du dépôt en temps normal et en cas de catastrophe, ainsi que les preuves relatives à la planification de la relève, soit les mesures en place pour assurer l'accès et la disponibilité des fonds de données, en ce moment et à l'avenir. Les évaluateurs cherchent des preuves que des préparatifs sont en place pour faire face aux risques inhérents aux changements de circonstances, y compris dans la mission ou la portée du dépôt.

Pour cette exigence, veuillez décrire :

- Le degré de responsabilité assumé pour les fonds de données, y compris toute période de préservation garantie ;
- Les plans à moyen terme (trois à cinq ans) et à long terme (> cinq ans) mis en place pour garantir la disponibilité et l'accessibilité continues des données. En particulier, il faut décrire à la fois la réaction aux changements rapides de circonstances et la planification à long terme, en indiquant les options de relocalisation ou de transition de l'activité vers une autre entité ou de restitution des fonds de données à leurs propriétaires (c'est-à-dire aux producteurs de données). Par exemple, qu'arrive-t-il en cas d'arrêt du financement pouvant être le résultat d'un retrait inattendu du financement, d'un arrêt planifié du financement d'un dépôt de projets limité dans le temps ou d'un changement d'intérêt de l'établissement hôte ?

Les preuves de cette exigence doivent porter particulièrement sur la gouvernance. Les aspects techniques de la continuité des activités et de la planification des catastrophes et de la succession doivent être couverts dans la section R15 (Infrastructure technique).

### Directives étendues R3.

Les évaluateurs recherchent des informations permettant de comprendre le degré de responsabilité assumé pour les données, le degré de risque pour l'organisation actuelle et le degré de planification de la relève pour l'avenir de la collecte des données. Par exemple, le demandeur est-il le principal ou le seul dépositaire ? Le déposant partage-t-il la responsabilité de l'avenir des données ? Le dépôt fournit-il l'accès, la préservation ou le stockage de données à un seuil de qualité minimum pendant une période minimum ? Cette information aide les évaluateurs à déterminer si le dépôt est viable en termes de finances et de processus, surtout en ce qui concerne la continuité de ses collections et de ses responsabilités en cas d'interruption temporaire ou permanente du service.

La responsabilité de la pérennité peut ne pas incomber au dépôt lui-même, mais à une organisation hôte ou apparentée. Le cas échéant, il faut l'indiquer clairement. De plus, si le dépôt fait partie d'une plus grande organisation, celle-ci ou une autre organisation (p. ex. des archives nationales) a-t-elle garanti qu'elle prendrait en charge cette responsabilité en cas d'interruption du service ? S'il n'y a pas d'accord formel et écrit entre le dépôt et l'organisation en question, le degré de conformité ne peut pas dépasser 3.

## 4. Confidentialité/éthique

**R4. Le dépôt garantit, dans la mesure du possible, que les données sont créées, traitées, accessibles et utilisées dans le respect des normes disciplinaires et éthiques.**

Degré de conformité :

**Réponse**

### Directives :

Le respect des normes éthiques est essentiel à une science responsable. Le risque de divulgation — par exemple, le risque qu'une personne ayant participé à une enquête puisse être identifiée ou que l'emplacement précis d'une espèce menacée puisse être localisé — est une préoccupation à laquelle de nombreux dépôts doivent aborder. Les preuves doivent démontrer que le dépôt a de bonnes pratiques pour les données comportant des risques de divulgation, y compris des conseils pour les déposants et les utilisateurs. Ces bonnes pratiques sont nécessaires pour maintenir la confiance de ceux qui acceptent que des données personnelles/sensibles soient stockées dans le dépôt.

Pour cette exigence, les réponses doivent inclure des preuves liées aux questions suivantes :

- Comment le dépôt se conforme-t-il aux normes disciplinaires en vigueur ?
- Le dépôt exige-t-il la confirmation que la collecte ou la création des données a été effectuée conformément aux critères juridiques et éthiques prévalant dans la situation géographique ou la discipline du producteur de données (p. ex. comité de révision éthique/conseil de révision institutionnelle ou législation sur la protection des données) ?
- Des procédures spéciales sont-elles appliquées pour gérer les données comportant un risque de divulgation ?
- Les données comportant un risque de divulgation sont-elles gérées de manière appropriée pour en limiter l'accès ?
- Les données comportant un risque de divulgation sont-elles distribuées dans des conditions appropriées ?
- Des procédures sont-elles en place pour examiner le risque de divulgation des données et pour prendre les mesures nécessaires soit pour anonymiser les fichiers, soit pour fournir un accès de manière sécurisée ?
- Le personnel est-il formé pour la gestion des données comportant un risque de divulgation ?
- Des mesures sont-elles en place si les conditions ne sont pas respectées ?
- Le dépôt fournit-il des conseils sur le versement, le téléchargement et l'utilisation responsables des données comportant un risque actuel ou potentiel de divulgation ?

Cette exigence concerne les dispositions en matière d'éthique et de confidentialité qui ont un impact sur la création, la curation et l'utilisation des données. Les détails des licences conformes à ces dispositions en matière d'éthique et de confidentialité doivent être couverts dans la section R2 (Licences).

## Directives étendues R4.

Toutes les organisations responsables des données ont le devoir éthique de les gérer selon les normes attendues par la pratique scientifique de sa communauté désignée. Pour les dépôts comportant des données sur des personnes, des organisations ou des zones et des espèces protégées, il y a des attentes légales et éthiques supplémentaires concernant la protection des droits des sujets des données.

La divulgation de ces données pourrait également présenter un risque de préjudice personnel, de violation de confidentialité commerciale ou de divulgation d'informations critiques (p. ex. la localisation d'espèces menacées ou d'un site archéologique). S'il y a un risque que des données identifiables soient déposées, de manière accidentelle par exemple, les responsables du dépôt doivent prendre des mesures appropriées pour traiter ces données et s'assurer qu'elles sont gérées (supprimées) conformément aux dispositions légales.

Le degré de conformité doit être de 4 si le dépôt donne actuellement accès à des données personnelles ou à d'autres données sensibles.

Les preuves doivent démontrer que les demandeurs comprennent leur environnement juridique et les pratiques éthiques pertinentes et qu'ils ont mis en place des procédures documentées pour assurer la conformité.

## 5. Infrastructure organisationnelle

**R5. Le dépôt dispose d'un financement adéquat et d'un personnel qualifié en nombre suffisant, géré par un système de gouvernance clair, pour mener à bien sa mission.**

Degré de conformité :

**Réponse**

### Directives :

Les dépôts ont besoin de fonds pour s'acquitter de leurs responsabilités, ainsi que d'un personnel compétent ayant une expertise dans l'archivage des données. Cependant, on convient également que la continuité du financement est rarement garantie ; cette incertitude doit être compensée en fonction du besoin de stabilité.

Pour cette exigence, les réponses doivent inclure des preuves liées aux éléments suivants :

- Le dépôt est hébergé par un établissement reconnu (assurant la stabilité et la durabilité à long terme) approprié pour sa communauté désignée.
- Le dépôt dispose d'un financement suffisant, y compris des ressources en personnel, des ressources informatiques et un budget pour assister aux réunions si nécessaire pour une période de trois à cinq ans idéalement.
- Le dépôt veille à ce que son personnel ait accès à de la formation continue et à du perfectionnement professionnel.
- L'étendue et le degré d'expertise tant de l'organisation que de son personnel, y compris toute affiliation pertinente (p. ex., organismes nationaux ou internationaux), sont convenables pour la mission.

Des descriptions complètes des tâches exécutées par le personnel du dépôt — et des compétences nécessaires pour les exécuter — peuvent être fournies, si elles sont disponibles. Ces descriptions ne sont toutefois pas obligatoires, car ce niveau de détail dépasse le cadre de la certification de base.

L'accès à des conseils objectifs d'experts au-delà de ceux fournis par le personnel qualifié est couvert dans la section R6 (Conseils d'experts).

### Directives étendues R5.

La réponse à cette exigence doit contenir des preuves décrivant les processus décisionnels en matière de gouvernance/gestion de l'organisme et les entités concernées. Le personnel doit avoir une formation appropriée en gestion des données afin de garantir des normes de qualité cohérentes. Il faut aussi savoir quelle proportion du personnel est employée de manière permanente ou temporaire et comment cette proportion peut affecter la qualité professionnelle du dépôt, surtout pour la préservation à long terme.

Dans quelle mesure le financement est-il structurel ou basé sur des projets ? Est-ce que cet arrangement peut être exprimé en nombre d'équivalent à temps plein.

Quelle est la fréquence du renouvellement périodique du financement ?

## 6. Directives d’experts

**R6. Le dépôt adopte des mécanismes pour obtenir des directives et des commentaires d'experts (internes ou externes, y compris des directives scientifiques, le cas échéant).**

Degré de conformité :

**Réponse**

### Directives :

Un dépôt efficace doit s'adapter à l'évolution des types, des volumes et des débits de données ainsi qu'adopter les nouvelles technologies les plus efficaces afin de conserver sa valeur pour la communauté désignée. Compte tenu de la rapidité des changements, on conseille aux responsables de dépôts de chercher régulièrement des conseils et des commentaires de la part d'utilisateurs experts afin d'assurer la pertinence et l'amélioration continues des données.

Pour cette exigence, les réponses doivent inclure des preuves liées aux questions suivantes :

- Le dépôt a-t-il des conseillers internes ou un comité consultatif externe qui pourrait être composé d'experts de la technique, de la curation, de la science des données et de la discipline ?
- Comment le dépôt communique-t-il avec les experts pour obtenir des conseils ?
- Comment le dépôt communique-t-il avec sa communauté désignée pour obtenir des commentaires ?

Cette exigence vise à confirmer que les responsables du dépôt ont accès à des conseils d'experts objectifs en plus de ceux fournis par le personnel qualifié mentionné dans la section R5 (Infrastructure organisationnelle).

### Directives étendues R6.

Les évaluateurs recherchent des preuves que le dépôt est lié à un réseau d'expertise élargi pour démontrer l'accès à des conseils et à des directives tant pour ses activités quotidiennes que pour la surveillance de nouveaux défis potentiels qui se profilent à l'horizon (veille communautaire et technologique). Si une partie de ces informations a déjà été fournie dans la section « R0. Brève description de la communauté désignée » et « Autres informations pertinentes », les demandeurs doivent y faire référence.

# Gestion d’objets numériques

## 7. Intégrité et authenticité des données

### R7. Le dépôt garantit l'intégrité et l'authenticité des données.

Degré de conformité :

### Réponse

### Directives :

Les responsables du dépôt doivent prouver qu'ils utilisent un système de gestion des données et des métadonnées pour garantir l'intégrité et l'authenticité pendant les processus d'acquisition, de stockage d'archives et d'accès aux données. Cette exigence couvre l'ensemble du cycle de vie des données au sein du dépôt.

Pour protéger l'intégrité des données et des métadonnées, toutes les modifications intentionnelles apportées aux données et aux métadonnées doivent être documentées, y compris les justifications et les auteurs des modifications. Des mesures doivent être mises en place pour garantir la détection des modifications accidentelles ou non autorisées et la récupération des versions correctes des données et métadonnées.

L'authenticité couvre le degré de fiabilité des données originales déposées et de leur provenance, y compris la relation entre les données originales et celles diffusées, et le maintien ou non des relations existantes entre les jeux de données ou les métadonnées.

Pour cette exigence, les réponses sur l'intégrité des données doivent inclure des preuves liées aux éléments suivants :

- Description des contrôles permettant de vérifier qu'un objet numérique n'a pas été altéré ou corrompu (c'est-à-dire les contrôles de fixité) du versement à l'utilisation.
- Documentation de l'exhaustivité des données et des métadonnées.
- Des précisions sur la manière dont toutes les modifications apportées aux données et aux métadonnées sont consignées.
- Description de la stratégie de gestion des versions.
- Utilisation des normes et conventions internationales appropriées (qui doivent être spécifiées).

Les questions suivantes portent sur les preuves à l’appui de la gestion d’authenticité :

- Le dépôt est-il doté d'une stratégie pour les modifications de données ? Les producteurs de données sont-ils mis au courant de cette stratégie ?
- Le dépôt maintient-il des données de provenance et des journaux d'audit connexes ?
- Le dépôt maintient-il des liens vers les métadonnées et vers d'autres jeux de données ? Si oui, comment ?
- Le dépôt compare-t-il les propriétés essentielles de différentes versions d'un même fichier ? Si oui, comment ?
- Le dépôt vérifie-t-il l'identité des déposants ?

### Directives étendues R7.

Les évaluateurs bénéficieront d'une vue d'ensemble claire des processus et des outils utilisés pour garantir la protection de l'authenticité et de l'intégrité des données tout au long du cycle de vie de la curation — y compris l'envergure des pratiques manuelles et automatisées — ainsi qu'une vue d'ensemble claire de la manière dont ces processus, outils et pratiques sont documentés. Conformément à la définition des lignes directrices de l'exigence, les demandeurs peuvent trouver utile de répondre à chaque point séparément et de traiter l'intégrité et l'authenticité indépendamment (notez que la réponse doit être rédigée en texte intégral).

Les journaux d'audit, qui sont des enregistrements écrits des actions effectuées sur les données, doivent être décrits dans les preuves fournies.

## 8. Évaluation

**R8. Le dépôt prend en charge des données et des métadonnées en fonction de critères définis assurant leur pertinence et leur compréhensibilité pour les utilisateurs.**

Degré de conformité :

**Réponse**

### Directives :

La fonction d'évaluation est essentielle pour déterminer si les données répondent à tous les critères de sélection et pour assurer une gestion appropriée de leur préservation. L'évaluation et la réévaluation au fil du temps garantissent que les données restent pertinentes et compréhensibles pour la communauté désignée.

Pour cette exigence, les réponses doivent inclure des preuves liées aux questions suivantes :

- Le dépôt est-il doté d'une politique de développement de la collection pour guider la sélection des données à archiver ?
- Quelle approche est utilisée pour les données qui ne relèvent pas du profil de mission/collection ?
- Le dépôt est-il doté de procédures permettant de déterminer l'inclusion des métadonnées nécessaires à l'interprétation et à l'utilisation des données ?
- Existe-t-il une évaluation automatisée de la conformité des métadonnées aux schémas pertinents ?
- Quelle est l'approche du dépôt si les métadonnées fournies sont insuffisantes pour la préservation à long terme ?
- Le dépôt publie-t-il une liste des formats préférés ?
- Est-ce que des contrôles sont en place pour s'assurer que les producteurs de données respectent les formats préférés ?
- Quelle est l'approche adoptée à l'égard des données qui sont déposées dans des formats inadaptés ?
- Quel est le processus pour retirer des éléments de votre collection, en tenant compte des répercussions sur les identifiants pérennes existants ?

Cette exigence couvre les critères de sélection appliqués au moment du dépôt. La qualité des données et leur amélioration au cours du processus de curation doivent être couvertes dans la section R11 (Qualité des données).

### Directives étendues R8.

Les demandeurs doivent démontrer que des procédures sont en place pour garantir que seules les données appropriées à la politique de collecte sont acceptées. Le personnel du dépôt doit disposer de toutes les informations, procédures et connaissances spécialisées nécessaires pour assurer la préservation et l'utilisation à long terme, selon le cas, pour la communauté désignée.

Pour que la collection reste pertinente et utilisable par la communauté désignée — surtout en fonction de l'évolution de la technologie, de la culture ou de la législation (p. ex. protection des données ou droits de propriété intellectuelle) — il faudra peut-être revoir les critères de sélection au fil du temps et réévaluer les actifs numériques. Des politiques et des procédures documentées doivent être mises en place pour le retrait d'éléments d'une collection.

## 9. Procédures de stockage documentées

**R9. Le dépôt dispose de procédures documentées pour gérer le stockage archivistique des données.**

Degré de conformité :

**Réponse**

### Directives :

Les dépôts doivent stocker les données et les métadonnées à partir du point de dépôt, en passant par le processus de versement, jusqu'au point d'accès. Les dépôts qui font de la préservation numérique doivent offrir un « stockage d'archives » selon les modalités du Open Archival Information System ou OAIS (Système ouvert d'archivage d'information).

Pour cette exigence, les réponses doivent inclure des preuves liées aux questions suivantes :

- De quelle manière les procédures pertinentes sont-elles documentées et gérées ?
- Le dépôt permet-il de comprendre clairement tous les lieux de stockage et la manière dont ceux-ci sont gérés ?
- Le dépôt dispose-t-il d'une stratégie pour les copies multiples ? Le cas échéant, quelle est-elle ?
- Est-ce que des techniques de gestion des risques sont utilisées pour informer la stratégie ?
- Quels contrôles sont en place pour garantir la cohérence entre les copies d'archives ?
- Comment la détérioration des supports de stockage est-elle gérée et surveillée ?

Les détails sur la mise en œuvre technique du stockage doivent être couverts dans la R15 (Infrastructure technique), et les dispositions spécifiques pour la sécurité physique et logique dans la section R16 (Sécurité).

### Directives étendues R9.

Les évaluateurs cherchent à comprendre chacun des lieux de stockage qui soutiennent les processus de curation, la manière dont les données sont gérées convenablement dans chaque environnement et les processus en place pour surveiller et gérer les changements dans la documentation de stockage. Les procédures sont-elles documentées et normalisées de manière à ce que différents gestionnaires de données parviennent sensiblement au même résultat en effectuant les mêmes tâches séparément ? Les exemples de preuves peuvent comporter des diagrammes de flux de données couvrant les lieux de dépôt, de conservation et d'accès (ainsi que toute restriction d'accès). Pour le stockage d'archives, les preuves peuvent comprendre des descriptions des dispositions pour plusieurs sites (sur site, près du site, hors site), la combinaison des supports de stockage et toute redondance (y compris l'intégrité par des sommes de contrôle).

## 10. Plan de préservation

**R10. Le dépôt assume la responsabilité de la préservation à long terme et gère cette fonction de manière planifiée et documentée.**

Degré de conformité :

**Réponse**

### Directives :

Le dépôt, les déposants de données et la communauté désignée doivent comprendre le niveau de responsabilité assumé pour chaque élément versé dans le dépôt. Le dépôt doit disposer des droits nécessaires pour assumer ces responsabilités. On doit documenter les procédures et s'assurer qu'elles sont respectées.

Pour cette exigence, les réponses doivent inclure des preuves liées aux questions suivantes :

- Le dépôt dispose-t-il d'une approche documentée pour la préservation ?
- Est-ce que le niveau de responsabilité pour la préservation de chaque élément est compris ? Comment celui-ci est-il défini ?
- Est-ce que des plans liés quant à de futures migrations ou à des mesures similaires pour contrer la menace d'obsolescence sont en place ?
- Le contrat entre le déposant et le dépôt prévoit-il toutes les actions nécessaires pour assumer les responsabilités ?
- Le transfert de la détention et le transfert de responsabilité sont-ils clairs pour le déposant et le dépôt ?
- Le déposant a-t-il les droits de copier, de transformer et de stocker les éléments, ainsi que d'y donner accès ?
- Les actions pertinentes pour la préservation sont-elles précisées dans la documentation, notamment le transfert de détention, les normes d'information sur les dépôts et les normes sur les informations archivistiques ?
- Existe-t-il des mesures pour garantir que ces actions sont prises ?

Les droits concernant l'accès et l'utilisation des données ainsi que la surveillance de leur respect doivent être couverts dans la section R2 (Licences).

### Directives étendues R10.

Le terme « plan de préservation » fait référence à l'existence d'une approche documentée pour définir et mettre en œuvre des actions de préservation. Les exigences ne définissent pas ou ne font pas de distinction entre une politique, un plan, une stratégie ou un plan d'action de préservation.

Les évaluateurs rechercheront une documentation claire et gérée afin de garantir : (1) une approche organisée pour la préservation à long terme (2) un accès continu pour les types de données malgré les changements de format, et (3) une documentation suffisante pour soutenir la capacité d'utilisation par la communauté désignée. La réponse doit indiquer si le dépôt a défini des niveaux de préservation et, le cas échéant, comment ils sont appliqués. Le plan de préservation doit être géré de sorte que les changements apportés à la technologie des données et aux exigences des utilisateurs sont traités de manière stable et rapide.

Si les niveaux de préservation diffèrent entre les classes ou les collections d'articles, le demandeur doit expliquer les différences dans l'approche de préservation, ainsi que les critères appliqués pour déterminer le niveau de préservation. Cela peut s'avérer pertinent si, par exemple, la taille du fichier d'un objet ou la sensibilité des données qu'il contient détermine le nombre de copies redondantes effectuées ; ou si seulement les éléments déposés dans des formats préférés sont convertis en formats de préservation standard et sont transférés à l'avenir.

Si le demandeur ne fournit pas de lien à une approche de préservation documentée, son degré de conformité sera au maximum 3 et il devra en avoir une en place au moment de la prochaine révision.

## 11. Qualité des données

**R11. Le dépôt dispose d'une expertise appropriée pour garantir la qualité des données techniques et des métadonnées et la disponibilité d'informations suffisantes pour que les utilisateurs finaux puissent effectuer des évaluations liées à la qualité.**

Degré de conformité :

**Réponse**

### Directives :

Les dépôts doivent avoir suffisamment d'informations sur les données pour que la communauté désignée puisse évaluer la qualité des données. L'évaluation de la qualité est encore plus pertinente lorsque la communauté désignée est multidisciplinaire et que les utilisateurs n'ont pas nécessairement l'expérience nécessaire pour évaluer la qualité à partir des données uniquement. Les dépôts doivent avoir des mécanismes permettant d'évaluer l'exhaustivité et la qualité des données et des métadonnées.

Les données ou les métadonnées connexes peuvent avoir des problèmes de qualité liés à leur valeur de recherche, mais elles peuvent servir si les utilisateurs sont en mesure de prendre des décisions éclairées quant à leur pertinence à la documentation fournie.

Pour cette exigence, veuillez décrire :

- L'approche en matière de qualité des données et des métadonnées conférées au dépôt.
- Le dépôt dispose-t-il de contrôles de qualité pour garantir l'exhaustivité et la compréhensibilité des données déposées ? Le cas échéant, veuillez fournir des références aux normes de contrôle de la qualité et aux mécanismes de rapport acceptés par la communauté de pratique pertinente et inclure des détails sur la façon dont les problèmes sont réglés (p. ex. les données sont-elles renvoyées au fournisseur de données pour rectification, corrigées par le dépôt, notées sur leur qualité dans le fichier de données ou incluses dans les métadonnées d'accompagnement) ?
- La capacité de la communauté désignée à commenter ou à noter les données et les métadonnées.
- Le fait que des citations d'ouvrages connexes ou des liens vers des indices de citation soient fournis.

Cette exigence fait référence aux normes et à l'assurance de la qualité relatives aux données dans le cadre de la curation. Les critères de sélection sont couverts dans la section R8 (Évaluation).

### Directives étendues R11.

Le demandeur doit indiquer clairement dans sa réponse qu'il comprend les niveaux de qualité auxquels on peut raisonnablement s'attendre de la part des déposants. Les preuves doivent décrire comment la qualité sera assurée pendant la curation et les attentes de la communauté désignée en matière de qualité. Le dépôt et ses déposants doivent avoir des documents sur tous les domaines dans lesquels la qualité des données ou des métadonnées est inférieure à la norme attendue.

## 12. Flux de travail

**R12. L'archivage se fait selon des flux de travail définis, du versement à la diffusion.**

Degré de conformité :

**Réponse**

### Directives :

Pour assurer la cohérence des pratiques entre les jeux de données et les services et éviter les actions ponctuelles, les flux de travail doivent être définis en fonction des activités du dépôt et clairement documentés. Des dispositions pour la gestion du changement doivent être mises en place. Le modèle de référence du OAIS peut aider à spécifier les fonctions du flux de travail d'un dépôt.

Pour cette exigence, les réponses doivent inclure des preuves liées aux éléments suivants :

- Descriptions des flux de travail ou des processus opérationnels.
- Une communication claire aux déposants et aux utilisateurs sur le traitement des données.
- Les niveaux de sécurité et les incidences sur les flux de travail (confidentialité des sujets, etc.).
- La vérification qualitative et quantitative des résultats.
- Les types de données gérées et les incidences sur les flux de travail.
- Le traitement des décisions au sein des flux de travail (p. ex., transformation des données d'archives).
- La gestion du changement des flux de travail.

Cette exigence confirme que tous les flux de travail sont documentés.

### Directives étendues R12.

Les évaluateurs cherchent des preuves que le demandeur adopte une approche cohérente, rigoureuse et documentée pour gérer toutes les activités tout au long de ses processus et que les changements apportés à ces processus sont mis en œuvre, évalués, enregistrés et administrés de manière appropriée.

L'exigence ne nécessite pas de descriptions détaillées des flux de travail, mais cherche des preuves de la manière dont ces flux de travail sont documentés et de l'endroit où ils le sont.

## 13. Découverte et identification des données

**R13. Le dépôt permet aux utilisateurs de découvrir les données et de faire référence à celle-ci de manière cohérente avec des citations appropriées.**

Degré de conformité :

**Réponse**

### Directives :

La découverte efficace des données est la clé du partage des données. Une fois découverts, les jeux de données doivent pouvoir être référencés par des citations complètes, y compris des identifiants pérennes pour garantir l'accès aux données à l'avenir.

Pour cette exigence, les réponses doivent inclure des preuves liées aux questions suivantes :

- Le dépôt offre-t-il des fonctionnalités de recherche ?
- Le dépôt maintient-il un catalogue de métadonnées consultable selon des normes appropriées (internationalement reconnues) ?
- Avec quels systèmes d'identifiants permanents le dépôt fonctionne-t-il ?
- Le dépôt facilite-t-il le moissonnage des métadonnées par machine ?
- Le dépôt fait-il partie d'autres registres de ressources disciplinaires ou génériques ?
- Le dépôt offre-t-il des citations de données recommandées ?

### Directives étendues R13.

La réponse doit contenir des preuves que la curation des données et des métadonnées favorise la découverte d'objets numériques clairement définis et identifiés, et permet de les relier à des objets numériques connexes conformément aux normes du domaine. La communauté désignée doit savoir clairement comment les données sont citées de manière à ce que le crédit et l'attribution appropriés soient accordés aux personnes ou organisations qui ont contribué à leur

## 14. Réutilisation des données

**R14. Le dépôt permet la réutilisation des données au fil du temps en garantissant que les métadonnées appropriées sont disponibles pour faciliter la compréhension et l'utilisation des données.**

Degré de conformité :

**Réponse**

### Directives :

Les dépôts doivent faire en sorte que les données continuent d'être comprises et utilisées efficacement à l'avenir, malgré les changements technologiques et l'évolution de la base de connaissances de la communauté désignée. Cette exigence évalue les mesures prises pour assurer la réutilisation des données.

Pour cette exigence, les réponses doivent inclure des preuves liées aux questions suivantes :

- Quelles métadonnées sont fournies par le dépôt lors de l'accès aux données ?
- Comment le dépôt assure-t-il la compréhension continue des données ?
- Les données sont-elles fournies dans des formats utilisés par la communauté désignée ? De quels formats s'agit-il ?
- Des mesures sont-elles prises pour tenir compte de l'évolution possible des formats ?

Le concept de « réutilisation » est essentiel pour les environnements dans lesquels les résultats d'analyses secondaires sont déposés de nouveau dans un dépôt avec les données primaires, car la chaîne de provenance et les questions de droits associées peuvent ainsi devenir de plus en plus compliquées.

### Directives étendues R14.

Pour satisfaire à cette exigence, le demandeur doit démontrer une connaissance approfondie des scénarios de réutilisation et des besoins de la communauté désignée en termes de pratiques, d'environnement technique et de (respect des) normes applicables. L'évolution de la technologie ainsi que des méthodologies et des normes employées par la communauté désignée peut nécessiter de reconsidérer le format dans lequel les données sont diffusées. De même, des métadonnées appropriées de grande qualité, conformes à un schéma généralisé ou disciplinaire, jouent un rôle essentiel et doivent être mentionnées dans les preuves fournies. Cette dernière information est essentielle pour concevoir des processus de curation garantissant que les objets numériques restent compréhensibles et utilisables par la communauté désignée au fil du temps. Si un schéma de métadonnées généralisé (tel que Dublin Core ou DataCite) est utilisé uniquement, le demandeur doit fournir la preuve qu'il suffit pour que le contenu préservé reste compréhensible par la communauté désignée.

# Technologie

## 15. Infrastructure technique

**R15. Le dépôt fonctionne avec un système d'exploitation et d'autres logiciels d'infrastructures adéquatement soutenus et s'appuie sur des technologies matérielles et informatiques convenables aux services qu'il offre à sa communauté désignée.**

Degré de conformité :

**Réponse**

### Directives :

Les dépôts doivent fonctionner avec des infrastructures fiables et stables qui maximisent la disponibilité des services. De plus, le matériel et les logiciels qu'ils utilisent doivent être pertinents et convenables pour la communauté désignée et pour les fonctions qu'ils remplissent. Le modèle de référence du Open Archival Information System ou OAIS (Système ouvert d'archivage d'information) précise les fonctions des dépôts pour répondre aux besoins des utilisateurs.

Pour cette exigence, les réponses doivent inclure des preuves liées aux questions suivantes :

- Quelles normes le dépôt utilise-t-il pour les références ? S'agit-il de normes internationales ou communautaires ? À quelle fréquence sont-elles révisées ?
- Comment les normes sont-elles mises en œuvre ? Existe-t-il des écarts importants par rapport à la norme ? Veuillez expliquer, le cas échéant.
- Le dépôt dispose-t-il d'un plan de développement des infrastructures ? Le cas échéant, quel est-il ?
- Est-ce qu'un inventaire des logiciels est maintenu et la documentation du système est-elle disponible ?
- Un logiciel soutenu par la communauté est-il utilisé ? Le cas échéant, veuillez décrire.
- La disponibilité, la bande passante et la connectivité sont-elles suffisantes pour répondre aux besoins de la communauté désignée ?
- Le dépôt dispose-t-il d'un plan de catastrophe et d'un plan de continuité des activités ? En particulier, des procédures et des dispositions sont-elles en place pour assurer une récupération rapide ou une sauvegarde des services essentiels en cas de panne ? Le cas échéant, quelles sont-elles ?

Les aspects de gouvernance de la continuité des activités, de la planification en cas de catastrophe et de la planification de la relève doivent être traités dans la section R3 (Continuité d'accès). Les détails sur le processus de stockage doivent être couverts dans la section R9 (Procédures de stockage documentées). Les dispositions relatives à la sécurité sont couvertes dans la section R16 (Sécurité).

### Directives étendues R15.

Les flux de travail et les acteurs humains offrant des services de dépôt doivent être soutenus par une infrastructure technologique appropriée qui répond aux besoins de la communauté désignée et permet au dépôt de se rétablir en cas de catastrophe à court terme. Les évaluateurs cherchent des preuves que le demandeur comprend l'écosystème généralisé des normes, des outils et des technologies disponibles pour la gestion et la curation des données (de recherche), et qu'il a choisi des options qui correspondent aux exigences locales. Si possible, le demandeur doit le démontrer en utilisant un modèle de référence.

Voici des exemples de normes pertinentes : les normes de la Spatial Data Infrastructure (SDI), les normes de l'Open Geospatial Consortium (OGC), les normes du W3C ou celles de l'ISO.

Pour les diffusions de données en temps réel ou quasi réel, la connectivité aux réseaux publics et privés est-elle assurée 24 heures par jour avec une bande passante suffisante pour respecter les responsabilités mondiales et/ou régionales du dépôt ?

## 16. Sécurité

**R16. L'infrastructure technique du dépôt assure la protection de l'installation, de ses données, de ses produits, de ses services et de ses utilisateurs.**

Degré de conformité :

**Réponse**

### Directives :

Le dépôt doit analyser les dangers potentiels, évaluer les risques et créer un système de sécurité cohérent. Cette analyse doit définir des scénarios de dommages résultant d'actions malveillantes, d'erreurs humaines ou de défaillances techniques qui constituent une menace pour le dépôt et ses données, ses produits, ses services et ses utilisateurs. Elle doit mesurer la probabilité et l'incidence de tels scénarios, déterminer les niveaux de risque acceptables et les mesures à prendre pour contrer les menaces pesant sur le dépôt et sa communauté désignée. Cette analyse doit faire l'objet d'un processus continu.

Pour cette exigence, veuillez décrire :

- Votre système de sécurité informatique, les employés ayant des rôles liés à la sécurité (p. ex., les agents de sécurité) et les outils d'analyse des risques (p. ex., DRAMBORA[2]) que vous utilisez ;
- Les niveaux de sécurité requis et la manière dont ils sont pris en charge ;
- Toutes les procédures d'authentification et d'autorisation utilisées pour gérer l'accès aux systèmes utilisés (p. ex., Shibboleth, OpenAthens) en toute sécurité.

Les processus de stockage et l'infrastructure technique qui utilisent ces mesures de sécurité doivent être couverts respectivement dans la section R9 (Procédures de stockage documentées) et la section R15 (Infrastructure technique).

### Directives étendues R16.

Les évaluateurs cherchent des preuves que le demandeur comprend tous les risques techniques applicables au service offert à la communauté désignée ainsi qu'à l'environnement physique. Le demandeur doit démontrer qu'il a mis en place des mécanismes pour prévenir, détecter et répondre à un incident de sécurité.

De quelle manière la sécurité de l'infrastructure technique est-elle contrôlée par le dépôt, par l'établissement hôte ou l'établissement externe ? Qui en est responsable ?

Les procédures d'authentification et d'autorisation en place sont-elles suffisantes pour garantir la sécurité des fonds de données à chaque étape du flux de travail (p. ex. en exigeant une authentification à deux facteurs pour les données sensibles) ?

Quelles politiques de sécurité organisationnelles sont en place pour régir la sécurité de tous les systèmes, y compris la sécurité du réseau, les contrôles d'intrusion, la sécurité des installations physiques et la politique en matière de mots de passe ?

[2] https://www.repositoryaudit.eu/

# Commentaires des demandeurs

## Commentaires/rétroaction

Ces exigences ne sont pas considérées comme définitives et nous serions reconnaissants de votre contribution pour améliorer la procédure de certification CoreTrustSeal. Tous les commentaires sur la qualité des exigences, leur pertinence pour votre organisation, ou toute autre contribution, seront pris en compte dans les prochaines versions.

**Réponse**