# Aanvullende toelichting, versie 2.0


# CoreTrustSeal Trustworthy Data Repositories Requirements: Extended Guidance 2020-2022

**Nederlandse vertaling**

**Netwerk Digitaal Erfgoed, 2020**

# Inhoud

# Inleiding

Dit is de vertaling van de volledige tekst van de **CoreTrustSeal Trustworthy Data Repositories Requirements** 2020-2022 met enkele inleidende paragrafen over de achtergrond en algemene richtlijnen. De vertaling is een initiatief van het Netwerk Digitaal Erfgoed en is een hulpmiddel voor erfgoedinstellingen die aan het begin staan van een certificeringsproces. De tekst is bedoeld om de drempel om een dergelijk proces in te gaan te verlagen en de eerste stappen naar een formele certificering te vergemakkelijken. De vertaling volgt zo goed mogelijk de oorspronkelijke Engelse tekst voor wat betreft de gehanteerde terminologie. Daar waar in de oorspronkelijke tekst de term *Repository* gebruikt wordt, spreekt de Nederlandse vertaling van *digitaal archief*. Een uiteindelijke formele certificering is altijd een beschrijving van de eigen context en dient in het Engels gedaan te worden. Om die reden zijn de kopjes boven alle Requirements onvertaald gelaten: dan ziet u direct welke beschrijving bij welke Requirement hoort.

Behalve de CoreTrustSeal Requirements zelf, die onveranderd blijven voor de periode 2020-2022, bevat het document aanvullende toelichtingen ('Extended Guidance') voor reviewers en aanvragers van de CoreTrustSeal. Het kan zijn dat de aanvullende toelichtingen in de periode 2020-2022 worden aangepast, maar dit gebeurt alleen na goedkeuring door het bestuur van CoreTrustSeal. Verder bevat het document een verwijzing naar een in het Nederlands vertaalde begrippenlijst.

Het doel van het document is een consistente beoordeling van alle CoreTrustSeal-aanvragen. Het is in eerste instantie bedoeld voor de reviewers, maar het is ook nuttig voor de zelfevaluatie van de aanvragers.

# Achtergrond & Algemene richtlijnen

De *CoreTrustSeal Trustworthy Data Repositories Requirements* is een beschrijving van de kenmerken van betrouwbare digitale archieven. Alle Requirements zijn verplicht en worden elk apart beoordeeld. Er is gepoogd mogelijke doublures in de gevraagde bewijsstukken van elke Requirement tot een minimum te beperken, maar een zekere mate van overlapping is onvermijdelijk. De checklists (bijv. Repository Type, Curation Level) zijn niet uitputtend en kunnen in de toekomst worden aangepast. Ook aanvragers zelf kunnen 'overige' opties toevoegen.

Bij elke Requirement staat een toelichting met een beschrijving van de informatie en het bewijsmateriaal dat aanvragers voor een objectieve beoordeling moeten aanleveren.

Bij elke Requirement moet de aanvrager aangeven in hoeverre aan de Requirement wordt voldaan ('Compliance Level'):

0 – Niet van toepassing
1 – Het digitale archief heeft dit nog niet overwogen
2 – Het digitale archief heeft een theoretisch concept
3 – Het digitale archief bevindt zich in de implementatiefase
4 – De richtlijn is volledig in het digitale archief geïmplementeerd

De Compliance Levels zijn een vorm van zelfevaluatie: een aanvrager beoordeelt daarmee de eigen voortgang. De reviewers van de aanvraag bepalen compliance op basis van de antwoorden en de onderbouwing van de aanvrager. Als een aanvrager van oordeel is dat een Requirement niet van toepassing is (level 0), dan dient dit uitvoerig te worden onderbouwd. Compliance Level 1 en 2 zijn niet voldoende voor het behalen van een certificaat. Een certificaat wordt alleen toegekend als een aantal Requirements zich in de implementatiefase bevindt (Compliance Level 3).

Aanvragers moeten in de onderbouwing van hun antwoorden links opnemen naar online bewijsmateriaal. Het certificeringsproces vindt plaats zonder locatiebezoek. Dit betekent dat het publiek toegankelijke materiaal eenduidig bewijs moet zijn van een goede bedrijfsvoering van het digitale archief. Kort voordat de aanvraag wordt ingediend, dienen alle opgenomen URL's te worden gecontroleerd.

Alle antwoorden moeten in het Engels worden gesteld. Het zal niet altijd mogelijk zijn om reviewers en aanvragers qua taal en discipline aan elkaar te koppelen, maar dat is wel het streven. Het is niet verplicht om van elk bewijs een vertaling aan te leveren. Maar van bewijsmateriaal dat niet in het Engels is gesteld, moet in het desbetreffende antwoord wel een Engelstalige samenvatting worden gegeven.

Voor het verkrijgen van de CoreTrustSeal is het niet nodig om gevoelige informatie te verstrekken. Toch zijn er binnen het certificeringproces wel mogelijkheden om bewijsmateriaal met gevoelige informatie te delen.

De CoreTrustSeal is drie jaar geldig vanaf de datum van toekenning. Door nieuwe technologieën en veranderende behoeften bij gebruikers zijn digitale archieven weliswaar voortdurend in ontwikkeling, maar ingrijpende veranderingen zullen ze in die periode waarschijnlijk niet ondergaan. Een organisatie met een goede bedrijfsvoering en goed beheer van de informatieobjecten zou na drie jaar met minimale aanpassingen een nieuwe aanvraag moeten kunnen indienen, tenzij:

- de organisatie, de datacollectie of de Designated Community aanzienlijk is veranderd;
- de CoreTrustSeal Requirements zodanig zijn gewijzigd dat dit gevolgen heeft voor de aanvrager.

De CoreTrustSeal Requirements worden elke drie jaar herzien. Dit heeft geen gevolgen voor een goedgekeurde aanvraag. De nieuwe Requirements gelden dan pas vanaf een nieuwe aanvraag.

# Begrippenlijst

Ga voor uitleg van de belangrijkste begrippen naar de Core Trustworthy Data Repositories Requirements Glossary: https://doi.org/10.5281/zenodo.3632563 (Engelstalig). Er is ook een Nederlandstalige versie van de begrippenlijst: https://doi.org/10.5281/zenodo.4073684 (Nederlandstalig)

# Algemene aanvullende richtlijnen

## Inleiding: Algemeen

Elke drie jaar bewijsmateriaal herzien alleen ten behoeve van certificering is efficiënt noch effectief. Om in aanmerking te komen voor certificering of om een certificaat te behouden zou normaal beheer van alle informatie in een digitaal archief die nodig is om de diensten in stand te houden, voldoende moeten zijn. Sterker nog, digitale archieven met een goed onderbouwd beleid en heldere procedures staan garant voor onder andere consistente kwaliteit en het opvangen van het risico van personeelsverloop. Zij zouden daarom in feite alleen antwoorden voor de aanvraag van certificering hoeven te formuleren en publiekelijk toegankelijke versies van hun bewijsmateriaal hoeven te beheren.

Het kan zijn dat reviewers een ander Compliance Level voorstellen dan de aanvrager heeft ingevuld. Als ze het Compliance Level verlagen, dan leggen ze uit waarom. Heeft een Requirement een Compliance Level lager dan 4 dan wordt er bij hernieuwde certificering vanuit gegaan dat de aanvrager vooruitgang heeft geboekt.

Het is niet doenlijk om voor elk type digitaal archief een beschrijving in de Toelichting of Aanvullende toelichting op te nemen. Bovendien is het niet verplicht op alle onderdelen of vragen in de Requirements een antwoord te geven. Aanvragers dienen in hun antwoorden wel in te gaan op de kwesties die in de Toelichting zijn beschreven en dienen daarbij inzicht te verschaffen in hun situatie. Het eindoordeel over een Requirement is afhankelijk van de volledigheid en kwaliteit van het antwoord. Reviewers willen een duidelijke, open onderbouwing van de specifieke situatie van de aanvrager.

De in de Requirements gebruikte begrippen en termen zijn gebaseerd op het OAIS Reference Model. Het gebruik van OAIS-terminologie geeft reviewers meer inzicht in en duidelijkheid over de aanvraag. Vandaar het dringende advies aan aanvragers zich in het OAIS-model te verdiepen voordat ze de Requirements beantwoorden. Een nuttige inleiding op het OAIS Reference Model is het 2014 DPC Technology Watch Report 'The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition)' van Brian Lavoie (https://doi.org/10.7207/twr14-02)[1].

## Onvolledige informatie/ontoereikend bewijs

Voor het certificeringsproces van CoreTrustSeal is de onderbouwing van en het bewijsmateriaal bij de antwoorden van groot belang. Uitgangspunt is dat de kwaliteit van het publiek toegankelijke bewijsmateriaal in de loop der tijd verbetert. Aanvragen zijn moeilijker te beoordelen als de verstrekte informatie onvolledig, ontoereikend of onduidelijk is, als URL's niet werken, of als in bewijsmateriaal steeds kruisverwijzingen worden gegeven.

Of een reviewer wel of niet (goed) bekend is met een digitaal archief mag geen rol spelen bij de beoordeling van het beschikbare bewijsmateriaal. Het definitieve, publiek toegankelijke bewijsmateriaal moet zo helder zijn dat ook medewerkers van andere digitale archieven het begrijpen.

Van reviewers mag niet worden verwacht dat ze zelf op de website van de aanvrager op zoek moeten gaan naar bewijs. Als een reviewer over onvoldoende informatie beschikt om tot een oordeel te komen, dan wordt de aanvraag teruggestuurd met een toelichting waarom het bewijs ontoereikend is. Reviewers kennen in deze fase nog geen Compliance Level toe.

## Begrijpelijkheid documentatie

Reviewers en lezers van de definitieve openbare review moeten de antwoorden op de Requirements kunnen begrijpen zonder het ondersteunende bewijsmateriaal te hoeven lezen. Als bewijsmateriaal uit een of meer langere documenten bestaat of als een document als bewijs voor meer dan één Requirement wordt gebruikt, dan moet de aanvrager specificeren welke onderdelen relevant zijn en de desbetreffende informatie in het antwoord citeren of samenvatten.

## Niet-Engelstalige documentatie

Het is toegestaan om documentatie in andere talen dan Engels te gebruiken mits de inhoud ervan op een adequate en duidelijke manier wordt uitgelegd in een Engelstalige samenvatting. Voor bepaalde soorten documenten, zoals een lijst met voorkeursformaten, kan de samenvatting vrij kort zijn; andere documenten, zoals een preserveringsbeleid, moeten uitgebreider zijn.

[1] Zie het artikel van Barbara Sierman voor een heldere Nederlandstalige uitleg van het OAIS-model: https://www.kb.nl/sites/default/files/docs/sierman_oiasmodelned.pdf

## Gevoelige en andere interne documentatie

Voor CoreTrustSeal-certificering is het niet verplicht om vertrouwelijke, commercieel gevoelige of veiligheidsgevoelige informatie openbaar te maken. Dat geldt ook voor documenten die alleen op het intranet van een digitaal archief beschikbaar zijn. Het kan ook zijn dat bepaalde bedrijfsinformatie zowel gevoelige informatie als relevant bewijsmateriaal bevat voor het aanvragen van CoreTrustSeal-certificering. Dergelijke informatie kan dan vertrouwelijk naar de reviewers worden gestuurd. In de aanvraag[2] dienen dan de namen en de inhoud van de documenten te worden vermeld en beschreven. Van de aanvrager wordt wel verwacht dat deze na verloop van tijd relevant bewijs uit de vertrouwelijke stukken filtert, zodat een openbare versie van de aanvraag beschikbaar kan worden gesteld voor de volgende reviewronde.

Als bepaalde documentatie nog niet bestaat, in ontwikkeling is of momenteel alleen voor intern gebruik beschikbaar is (bijvoorbeeld een wiki), dan dient in de aanvraag een datum te worden vermeld waarop die documentatie vrij beschikbaar komt. Dit kan voldoende zijn voor goedkeuring van de aanvraag voor certificering. Voor verlenging van de certificering dient de aanvrager wel publiek toegankelijke documentatie aan te leveren.

## Structuur en omvang aanvraag

Reviewers en het bestuur van CoreTrustSeal behandelen alle aanvragen vertrouwelijk, maar zodra een aanvraag is goedgekeurd wordt deze openbaar gemaakt. Aanvragers dienen zich daarom bewust te zijn van alle mogelijke lezers. Het is niet de bedoeling dat elk onderdeel van de toelichting puntsgewijs wordt uitgelegd. Het antwoord op elke Requirement moet een lopende tekst zijn waarin relevante aspecten van de Toelichting en Aanvullende toelichting zijn uitgewerkt.

Het CoreTrustSeal-bestuur beseft dat allerlei soorten organisaties een aanvraag kunnen indienen. Ze kunnen variëren in missie, omvang en complexiteit, zowel qua organisatiestructuur als qua diversiteit van de datacollectie. Zelfs in de Aanvullende toelichting kan niet worden voorzien welk onderwerp of welk type bewijsmateriaal relevant is voor de aanvraag. We begrijpen ook dat er ruimte nodig is om de relevantie van bewijsmateriaal uit te leggen, met name van niet-Engelstalig bewijs. Aan de lengte van antwoorden is daarom geen minimum of maximum gesteld, maar de ervaring leert dat zelfs de meest ingewikkelde onderbouwingen niet langer hoeven te zijn dan 500 tot maximaal 800 woorden. Bewijs dient, indien mogelijk, vergezeld te gaan van openbare links naar documentatie waarin het beleid van de organisatie en van het beheer van de digitale objecten staan beschreven. Dit publiek toegankelijke bewijs is de allerbelangrijkste garantie dat een organisatie de eigen collecties als een Trustworthy digitaal archief beheert.

Het is niet noodzakelijk om bij verschillende Requirements lange passages uit andere antwoorden te herhalen. Bewijs dat relevant is voor meer dan één Requirement hoeft maar één keer volledig te worden gegeven. In de antwoorden bij andere Requirements kan dan worden volstaan met een korte samenvatting van de relevante informatie en een kruisverwijzing naar de desbetreffende Requirement.

[2] Stuur vertrouwelijke documenten naar het volgende e-mailadres van het CoreTrustSeal Secretariat: info@coretrustseal.org

# Requirements

## Achtergrondinformatie

## Context

**R0. Please provide context for your repository.**
*(Beschrijf de context van het digitaal archief.)*

**- Repository type. Select all relevant types from:**
*(Type digitaal archief. Kies alle relevante types.)*

- Domein- of onderwerpspecifiek digitaal archief
- Institutioneel digitaal archief
- Nationaal digitaal archief, inclusief overheid
- Digitaal archief voor publicaties
- Bibliotheek
- Museum
- Archief
- Digitaal archief voor onderzoeksprojecten
- Overig (Geef een beschrijving)

**- Brief Description of Repository**
(Beknopte beschrijving van het digitaal archief)

**- Brief Description of the Designated Community**
(Beknopte beschrijving van de gedefinieerde doelgroep)

**- Level of Curation Performed. Select all relevant types from:**
(Niveau van preservering. Kies alle relevante types:)

**A. Content distributed as deposited**
*(Content wordt beschikbaar gesteld zoals deze is gedeponeerd)*
**B. Basic curation - e.g., brief checking, addition of basic metadata or documentation**
(Basispreservering, met onder andere eenvoudige controles, toevoeging elementaire metadata of documentatie)
**C. Enhanced curation - e.g., conversion to new formats, enhancement of documentation**
*(Uitgebreide preservering, zoals het migreren naar nieuwe bestandsformaten en het verbeteren van documentatie)*
**D. Data-level curation - as in C above, but with additional editing of deposited data for accuracy**
*(Beheer op informatieniveau: zoals C hierboven, maar met aanvullende verrijking en correctie van gedeponeerde data)*

**Comments**
*(Opmerkingen)*

**- Insource/Outsource Partners. If applicable, please list them.**

(Vermeld alle samenwerkingspartners (zowel interne partners als uitbestedingspartners) indien van toepassing.)

**- Summary of Significant Changes Since Last Application (if applicable)**
(Samenvatting belangrijke veranderingen sinds vorige aanvraag, indien van toepassing)

**- Other Relevant Information**
(Overige relevante informatie)

## Antwoord

## Toelichting

Dit onderdeel bevat informatie over de achtergrond en de context die reviewers nodig hebben om de antwoorden op de volgende Requirements goed te kunnen beoordelen. Daarom is het van cruciaal belang dat u op elke vraag een zo gedetailleerd mogelijk antwoord geeft. Maak een keuze uit de gegeven opties en geef gedetailleerde informatie over de items in de Context Requirement.

***(1) Repository Type.*** Beschrijf de functie van het digitale archief. Kies het type dat het beste bij het digitale archief past (meerdere keuzes mogelijk). Is geen van de gegeven categorieën van toepassing? Voeg dan bij 'Other' (Overig) een ander type toe. Voeg indien nodig of wenselijk aanvullende informatie toe om reviewers beter inzicht te geven in het type digitaal archief.

***(2) Brief Description of Repository.*** Geef een beknopte beschrijving van het digitale archief. Beschrijf met name welk type data het digitale archief accepteert (reikwijdte van de collectie). Heeft het digitale archief outsource partners (uitbestedingspartners) of is het onderdeel van een netwerk of een grotere organisatie? Neem in het antwoord dan bij voorkeur een organigram op of een omschrijving van de overkoepelende organisatiestructuur.

***(3) Designated Community.*** Geef een duidelijke omschrijving van de Designated Community (Gedefinieerde doelgroep – zie Begrippenlijst: https://doi.org/10.5281/zenodo.4073684) waaruit blijkt dat u als aanvrager goed inzicht heeft in de reikwijdte, basiskennis en methodologieën (zoals voorkeurssoftware of -formaten) van de beoogde gebruikersgroep(en). Zorg ervoor dat het antwoord voldoende gedetailleerd is zodat reviewers kunnen bepalen of de curatie- en preserveringsmaatregelen zoals beschreven in de aanvraag toereikend zijn.

***(4) Level of Curation.*** Het doel van dit onderdeel is om te achterhalen of de content van het digitale archief onveranderd aan gebruikers beschikbaar wordt gesteld of dat die op een of andere manier is verrijkt. Bij alle niveaus van preservering wordt ervan uitgegaan (1) dat oorspronkelijke depots onveranderd zijn opgeslagen en dat eventuele wijzigingen alleen zijn doorgevoerd in kopieën van het origineel, en (2) dat metadata die de Designated Community in staat stellen data te begrijpen en te gebruiken zonder een beroep te hoeven doen op de oorspronkelijke maker, al in het depot aanwezig zijn of door het digitale archief zijn toegevoegd. Annotaties en wijzigingen zijn alleen toegestaan voor zover ze voldoen aan de voorwaarden van de met de dataproducent overeengekomen licentie en moeten duidelijk binnen de competenties vallen van degenen die verantwoordelijk zijn voor de curatie. Het uitgangspunt is dat het digitaal archief aantoont dat alle annotaties en/of wijzigingen worden uitgevoerd en vastgelegd door competente deskundigen en dat de integriteit van alle originele data behouden blijft. Dit helpt reviewers bij het beoordelen van andere Requirements voor certificering. Voeg indien nodig of wenselijk aanvullende informatie toe die reviewers meer inzicht geeft in de niveaus van preservering van het digitale archief.

***(5) Insource/Outsource Partners.*** Lever een overzicht aan van de partners waarmee de organisatie samenwerkt en beschrijf de aard van de relatie (organisatorisch, contractueel, enz.). Beschrijf ook of de partners zelf een certificeringstraject voor hun eigen digitaal archief hebben doorlopen. Als bepaalde functies of ondersteunend bewijsmateriaal niet onder direct beheer van de aanvrager vallen, dan moet dat hier worden vermeld en toegelicht. Hierbij kan het gaan om zowel een gastorganisatie of een andere vorm van interne samenwerking als uitbesteding of een ander soort afhankelijkheid van een derde partij. Voorbeelden van dergelijke relaties zijn (1) dienstverlening van een instelling waarvan uw organisatie deel uitmaakt, (2) opslagcapaciteit van derden als onderdeel van een beleid van redundante opslag, of (3) lidmaatschap van organisaties die het beheer van uw datacollectie voor hun rekening nemen op het moment dat de continuïteit onder druk staat. Lever ook een overzicht aan van de Requirements waarvoor de partner (een aantal) relevante functies/diensten levert. Denk hierbij aan relevante overeenkomsten en SLA's (Service Level Agreements). Omdat nagenoeg altijd sprake zal zijn van gedeeltelijke uitbesteding zal relevant bewijsmateriaal moeten worden aangeleverd voor Requirements die niet worden uitbesteed en voor de onderdelen van de levenscyclus van data die onder het eigen beheer van het digitale archief vallen. Uitbestedingspartners zijn bij voorkeur in het bezit van kwalificaties en certificeringen zoals die van CoreTrustSeal en haar voorgangers. Dit is echter niet verplicht. We begrijpen dat het moeilijk is al deze informatie boven water te krijgen, maar die is wel van essentieel belang voor een compleet en sluitend reviewproces.

***(6) Summary of Significant Changes Since Last Application.*** Bij CoreTrustSeal-certificering wordt ervan uitgegaan dat u permanent aan verbetering van het digitale archief werkt. Bij een aanvraag voor hercertificering dient een beknopte beschrijving te worden gegeven van onder andere eventuele grote wijzigingen in de technische systemen, Designated Community en financiering in de afgelopen drie jaar. Verwijs hierbij naar mogelijke opmerkingen van reviewers in de voorgaande CoreTrustSeal-aanvraag. Voeg gedetailleerde informatie over wijzigingen toe aan het antwoord bij de desbetreffende Requirement.

***(7) Other Relevant Information.*** Het is mogelijk om aanvullende contextuele informatie te verschaffen die niet expliciet in de Requirements is vermeld maar die wel relevant kan zijn voor de reviewers. Denk hierbij bijvoorbeeld aan:

- het gebruik en de impact van databestanden in het digitale archief (citaten, gebruik in andere projecten, enzovoorts);
- nationale, regionale of mondiale functies van het digitale archief;
- samenwerkingsverbanden of netwerken waarvan het digitale archief onderdeel uitmaakt.

# Aanvullende toelichting R0.

## Repository Type & Brief Description of Repository

Heeft u meer dan één type digitaal archief geselecteerd? Geef dan bij *Brief Description of Repository* een toelichting waarmee u duidelijk maakt hoe die verschillende functies worden gerealiseerd. In die toelichting kunt u verwijzen naar relevante datacollecties, datatypes, formaten en disciplines waarmee het digitale archief werkt.

## Brief Description of the Designated Community

Zoals blijkt uit de definitie van het begrip 'Designated Community' (zie de Begrippenlijst: https://doi.org/10.5281/zenodo.4073684) kan een digitaal archief meerdere soorten gebruikersgroepen hebben, bijvoorbeeld voor verschillende collecties. Geef in dat geval een definitie en een voldoende gedetailleerde beschrijving van elke gebruikersgroep. Belangrijk hierbij is dat de Designated Community kleiner in omvang kan zijn dat het totaal aan gebruikers. De digitale collecties van een natuurhistorisch

museum zijn bijvoorbeeld misschien interessant voor een grote groep geïnteresseerde gebruikers of het grote publiek, maar het museum zelf kan een veel engere definitie van de Designated Community hanteren, bijvoorbeeld biologen of antropologen die onderzoek doen naar natuurhistorische onderwerpen.

Om een Designated Community goed van dienst te kunnen zijn, moet een digitaal archief goed inzicht hebben in de samenstelling, vaardigheden, basiskennis en behoeften van de Designated Community en hoe deze in de loop der tijd kunnen veranderen. Uit het aangeleverde bewijsmateriaal in de aanvraag moet blijken dat bij het digitaal archief voldoende kennis en inzicht aanwezig is over de eisen waaraan preservering moet voldoen (aanvullende context, voorkeursformaten, enzovoorts) om de Designated Community (en eventuele gebruikersgroepen) zo goed mogelijk van dienst te zijn. Daarnaast moet de aanvrager aantonen dat veranderingen in de behoeften van de Designated Community worden gemonitord en dat hierop wordt ingespeeld.

Voor een digitaal archief met een uiterst specifieke, eng gedefinieerde Designated Community is het wellicht eenvoudig om de veronderstelde basiskennis van die doelgroep te formuleren (bijvoorbeeld kennis van genetica of het gebruik van statistische software). Maar voor een bredere Designated Community, bijvoorbeeld een doelgroep die uit meerdere gebruikersgroepen bestaat, moet een digitaal archief voldoende inzicht in de basiskennis van al die gebruikersgroepen hebben en een breed pakket aan contextuele documentatie verschaffen om er zeker van te zijn dat iedereen binnen de Designated Community de data begrijpt. Expliciteer daarom in de definitie van de basiskennis van de Designated Community welke onderliggende kennis als bekend wordt verondersteld, zoals (vreemde)talenkennis of vertrouwdheid met en toegang tot specifieke besturingssystemen, internetbrowsers of software.

## Level of Curation Performed

Kies hier een of meer niveaus van preservering: A, B, C en/of D. De keuze hangt af van het type data in het digitale archief en van de met de depotgever overeengekomen voorwaarden. Wordt een digitaal archief op meer dan één niveau beheerd, dan moet u uitleggen welke data in de collectie op welk niveau worden beheerd. Uit de antwoorden op de Requirements moet dan blijken hoe de workflows van het beheer een afspiegeling vormen van de verschillende niveaus en hoe deze zich verhouden tot de preserveringsniveaus. Zo moet bijvoorbeeld duidelijk worden gemaakt of de preserveringsdoelen en -acties voor alle data gelijk zijn, onafhankelijk van het desbetreffende preserveringsniveau.

Geef niet alleen een beschrijving van de preserveringsniveaus, maar toon ook aan dat er sprake is van duurzame toegankelijkheid van de data, ook als de behoeften van de Designated Community veranderen. De kans dat dit op curatieniveau A en B gebeurt, is minder waarschijnlijk, omdat zonder normalisering van de aangeleverde bestandsformaten naar een standaard preserveringsformaat bij toekomstige formaatmigraties de nodige problemen zouden kunnen ontstaan als gevolg van de heterogeniteit van de collectie. Maar ook een gebrek aan rijke metadata en documentatie kan een risico vormen voor duurzaam gebruik van de data.

Hoe hoger het preserveringsniveau (A-D), hoe groter de verwachtingen van de reviewers ten aanzien van het niveau van formele herkomst, integriteit en versiebeheer (wijzigingslog, e.d.).

## Insource/Outsource Partners

Is er sprake van meer dan één partner, voeg dan een schema toe met een overzicht van het volledige proces van interne samenwerking en/of uitbesteding. Een digitaal archief met meerdere samenwerkingspartners (intern en/of extern, bijvoorbeeld één partner voor dataopslag en een andere die de website beheert) is geen probleem mits alle relaties inzichtelijk worden gemaakt. Reviewers vragen om herformulering van het antwoord in dit onderdeel als in onderbouwingen verderop in de aanvraag wordt verwezen naar entiteiten die hier niet zijn vermeld.

## Other Relevant Information

Hier kunt u eventueel verwijzen naar bijvoorbeeld registratie in re3data (http://www.re3data.org/), het aantal medewerkers, de omvang van de collectie, het gemiddelde aantal downloads, de chronologische ontwikkeling van het digitale archief en/of het bedrijfs- of financieringsmodel. Een heldere, consistente omschrijving van de hele organisatorische aanpak wordt door de reviewers over het algemeen als nuttig ervaren.

# Organisatorische infrastructuur

## 1. Mission/Scope

### R1. The repository has an explicit mission to provide access to and preserve data in its domain.

(Een expliciete missie van het digitale archief is het toegankelijk maken en preserveren van data binnen een specifiek domein.)

Compliance Level:

**Antwoord**

### Toelichting

Digitale archieven zijn de beheerders van digitale objecten en zijn verantwoordelijk voor het bewaren van materialen in een daarvoor passende omgeving gedurende een vastgestelde termijn. Voor depotgevers en gebruikers moet duidelijk zijn dat het preserveren en toegankelijk houden van de data een expliciete taak van het digitale archief is.

Geef voor deze Requirement een beschrijving van:

- de missie van uw organisatie ten aanzien van het preserveren en toegankelijk houden van data, inclusief links die expliciet naar uitingen van deze missie verwijzen;
- de mate waarin de missie binnen de organisatie wordt gedragen.

Het bewijsmateriaal bij het antwoord op deze Requirement zou kunnen bestaan uit bijvoorbeeld (1) een goedgekeurde en gepubliceerde missie, (2) een beschrijving van door financiers toegewezen rollen en (3) een door de raad van toezicht ondertekende beleidsplan.

### Aanvullende toelichting R1.

Als in de missie van het digitale archief niets vermeld staat over de preservering van data, dan is Compliance Level 3 of 4 voor deze Requirement uitgesloten.

# 2. Licenses

## R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.

(Het digitale archief beschikt over alle toepasselijke licenties voor toegang tot en gebruik van de data en bewaakt de naleving van de licentievoorwaarden.)

Compliance Level:

### Antwoord

### Toelichting

Een digitaal archief beschikt over een toepasselijk rechtenmodel voor toegang tot en gebruik van de data, communiceert daarover met de gebruikers en bewaakt de naleving van de licentievoorwaarden. Deze Requirement heeft betrekking op zowel de toegangsvoorwaarden en van toepassing zijnde licenties van het digitale archief zelf als algemeen geaccepteerde gedragsregels voor de uitwisseling en het correcte gebruik van kennis en informatie in het relevante domein. Uit het bewijsmateriaal moet duidelijk blijken dat het digitale archief over voldoende controle-instrumenten beschikt voor het toetsen van de toegangscriteria tot de data en dat alle relevante licenties en processen goed worden beheerd.

Geef voor deze Requirement een beschrijving van:

- alle geldende licentieovereenkomsten;
- gebruiksvoorwaarden (intellectueel eigendom, distributie, gebruiksdoel, bescherming gevoelige informatie, enzovoorts);
- documentatie over te nemen maatregelen bij schending van toegangs- en gebruiksvoorwaarden.

Wanneer alle data volledig openbaar zijn en zonder voorwaarden aan gebruikers beschikbaar worden gesteld (bronvermeldingen zijn bijvoorbeeld niet verplicht en secundaire analyses hoeven niet vrij toegankelijk te zijn), dan kan dit worden vermeld.

Ethische en privacy-gerelateerde bepalingen met gevolgen voor licenties komen aan bod in R4 (Confidentiality/Ethics). Bij R10 (Preservation Plan) dient de garantie te worden gegeven dat het digitale archief met de overeengekomen archiveringsovereenkomst over voldoende bevoegdheden beschikt voor het beheren, preserveren en toegankelijk maken van data.

### Aanvullende toelichting R2.

Bepalingen over de toegang tot en het gebruik van data kunnen in algemene voorwaarden worden vastgelegd of per depotgever of dataset worden uitgesplitst. Met name voor gevoelige data kunnen in licenties specifieke bepalingen worden opgenomen over gebruiksbeperkingen, gebruiksomgevingen (zoals speciale ruimtes en secure remote access) en soorten gebruikers (zoals goedgekeurde onderzoekers en gebruikers met een speciale opleiding). Voorbeelden van veelgebruikte licentie-opties zijn die van Creative Commons (https://creativecommons.org/) zoals 'CC 0 Waiver'- en 'public domain data'-licenties.

Schendingen van licentievoorwaarden zijn misschien niet gemakkelijk te bepalen. Toch is het belangrijk om bij deze Requirement aandacht te schenken aan de gevolgen van dergelijke schendingen, bijvoorbeeld met een beschrijving van sancties ten aanzien van de toegang tot of het gebruik van data nu of in de toekomst. Het openbaar maken van gevoelige persoonlijke informatie kan leiden tot zware juridische sancties met gevolgen

voor zowel de gebruiker als het digitale archief. Het digitale archief heeft bij voorkeur een gepubliceerd beleid voor schending van licenties en licentievoorwaarden.

Als het digitale archief op dit moment toegang verleent tot persoonlijke gegevens, dan is Compliance Level 4 verplicht.

# 3. Continuity of access

## R3. The repository has a continuity plan to ensure ongoing access to and preservation of its holdings.

(Het digitale archief heeft een continuïteitsplan om ervoor te zorgen dat de collectie altijd toegankelijk zijn en gepreserveerd blijft.)

Compliance Level:

### Antwoord

### Toelichting

Bij deze Requirement gaat het over de manier(en) waarop het digitaal archief ervoor zorgt dat de collectie altijd, ook tijdens rampspoed, toegankelijk blijft. Tevens gaat het over de onderbouwing van het continuïteitsplan, d.w.z. dat er maatregelen zijn getroffen om te waarborgen dat de collectie altijd toegankelijk en beschikbaar is, zowel nu als in de toekomst. Reviewers willen bewijs zien dat er voorbereidingen zijn getroffen om de risico's van veranderende omstandigheden, zoals veranderingen in de missie of scope van het digitale archief, het hoofd te kunnen bieden.

Geef voor deze Requirement een beschrijving van:

- de aard van de verantwoordelijkheid voor de collectie, zoals de gegarandeerde duur van preserveringstermijn;
- de middellange- (drie tot vijf jaar) en langetermijnplannen (meer dan vijf jaar) voor gegarandeerde beschikbaarheid en toegankelijkheid van de collectie. Beschrijf met name hoe wordt ingespeeld op snel veranderende omstandigheden en wat de langetermijnplannen zijn. Maak daarbij duidelijk welke opties er zijn om de activiteiten aan een andere partij over te dragen of om de collectie aan de eigenaar (de maker of depotgever) terug te geven. Leg bijvoorbeeld uit wat er gebeurt als de financiering wordt beëindigd, d.w.z. als die onverwacht wordt stopgezet of als de looptijd volgens planning afloopt. Het kan ook zijn dat de host het eigen beleid verandert. Hoe wordt daarmee omgegaan?

Zorg ervoor dat de onderbouwing van het antwoord op deze Requirement is toegespitst op goed bestuur en toezicht. De technische aspecten van de bedrijfscontinuïteit, het rampenplan en het continuïteitsplan komen aan bod in R15 (Technical infrastructure).

### Aanvullende toelichting R3.

Reviewers willen inzicht hebben in de mate van verantwoordelijkheid voor de data, in het risiconiveau voor de huidige organisatie en in de kwaliteit van het continuïteitsplan voor de toekomst van de datacollectie. Is de aanvrager bijvoorbeeld de primaire of enige beheerder? Is de depotgever mede-verantwoordelijk voor de toekomst van de data? Garandeert het digitale archief de toegankelijkheid, preservering en/of opslag van data tot op een bepaald minimum kwaliteitsniveau voor een bepaalde minimum termijn? Op basis van deze informatie kunnen reviewers beoordelen of het digitale archief duurzaam is wat betreft financiering en processen, in het bijzonder wat betreft de continuïteit van de collecties en verantwoordelijkheden bij een tijdelijke of permanente onderbreking van de dienstverlening.

Mogelijkerwijs ligt de verantwoordelijkheid voor de duurzaamheid niet bij het digitale archief zelf maar bij een gastorganisatie of een bovenliggende organisatie. Zo ja, dan dient dat duidelijk te worden aangegeven. En als

het digitale archief onderdeel is van een grotere organisatie dan is de vraag of die organisatie (of een andere organisatie, zoals een nationaal archief) bij een eventuele onderbreking van de continuïteit van de dienstverlening garant staat voor het overnemen van de verantwoordelijkheid. Zonder formele schriftelijke overeenkomst tussen het digitale archief en een dergelijke organisatie is het Compliance Level maximaal 3.

# 4. Confidentiality/Ethics

## R4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.

(Het digitale archief zorgt ervoor dat bij de totstandkoming, het beheer, de toegang en het gebruik van de data zo veel mogelijk rekening wordt gehouden met domeinspecifieke normen en gedragsregels.)

Compliance Level:

### Antwoord

### Toelichting

Naleving van gedragsregels is van cruciaal belang voor verantwoorde wetenschap en verantwoord collectiebeheer. Het risico van openbaarmaking, zoals het risico dat persoonlijke gegevens van een deelnemer aan een enquête of de precieze locatie van een bedreigde diersoort bekend worden, is een kwestie die veel digitale archieven aangaat. Uit de onderbouwing van het antwoord moet blijken dat het digitale archief goede maatregelen heeft getroffen voor de bescherming van persoonlijke en gevoelige data en dat het depotgevers en gebruikers hier ook goede ondersteuning bij biedt. Dit is nodig voor het vertrouwen van degenen die zich bereid hebben verklaard persoonlijke/gevoelige informatie aan het digitale archief toe te vertrouwen.

Neem in de onderbouwing van het antwoord op deze Requirement onder andere de volgende vragen mee:

- Hoe zorgt het digitale archief voor naleving van toepasselijke domeinspecifieke normen?
- Vraagt het digitale archief om bevestiging dat data zijn verzameld of tot stand zijn gekomen conform de wettelijke en ethische criteria die van toepassing zijn op het geografische gebied of de discipline van de maker of depotgever (bijv. ethische toetsingscommissie, institutionele toetsingscommissie, wetgeving gegevensbescherming)?
- Zijn er specifieke procedures voor het beheren van (privacy)gevoelige data?
- Worden (privacy)gevoelige data zodanig beheerd dat toegang ertoe beperkt is?
- Verloopt de distributie van (privacy)gevoelige data volgens de toepasselijke voorwaarden?
- Zijn er procedures voor het beoordelen van (privacy)gevoelige data en voor het treffen van maatregelen voor het anonimiseren van bestanden of voor veilige toegang tot data?
- Is het personeel opgeleid voor het beheer van (privacy)gevoelige data?
- Zijn er maatregelen getroffen voor het geval er niet aan de voorwaarden of procedures wordt voldaan?
- Biedt het digitale archief ondersteuning voor het verantwoord aanleveren, downloaden en gebruiken van (mogelijk) (privacy)gevoelige data?

In deze Requirement gaat het om gedragsregels en privacybepalingen die van invloed zijn op de totstandkoming, de curatie en het gebruik van data. Informatie over licenties in verband met dergelijke gedragsregels en privacybepalingen dient bij R2 (Licenses) te worden gegeven.

### Aanvullende toelichting R4.

Alle organisaties met een verantwoordelijkheid voor data hebben een morele plicht die data zodanig te beheren dat het niveau van dat beheer voldoet aan de wetenschappelijke normen van de Designated Community. Voor digitale archieven met data van individuen, organisaties of beschermde onderwerpen of soorten gelden aanvullende wettelijke en ethische normen ten aanzien van de bescherming van hun rechten.

Openbaarmaking van deze data zou kunnen leiden tot persoonlijke schade, schending van commerciële vertrouwelijkheid of bekendmaking van cruciale informatie zoals de locatie van een bedreigde diersoort of een archeologische site. Als er een risico bestaat dat er bijvoorbeeld per ongeluk traceerbare data worden aangeleverd, dan dient het digitale archief passende maatregelen te treffen voor de verwerking (en verwijdering) van die data. Dit dient te gebeuren conform wet- en regelgeving.

Als het digitale archief momenteel toegang biedt tot persoonlijke of andere gevoelige data dan is Compliance Level 4 vereist.

Uit de onderbouwing moet blijken dat de aanvrager inzicht heeft in het wettelijk kader en de relevante gedragsregels en hiervoor ook gedocumenteerde procedures heeft vastgelegd om naleving af te dwingen.

# 5. Organizational infrastructure

## R5. The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.

(Het digitale archief beschikt over voldoende financiële middelen en voldoende gekwalificeerd personeel dat op een heldere manier wordt aangestuurd voor een doeltreffende uitvoering van de missie.)

Compliance Level:

### Antwoord

### Toelichting

Digitale archieven hebben niet alleen financiële middelen nodig voor de uitvoering van hun verantwoordelijkheden, maar ook deskundig personeel met ervaring op het gebied van archivering van data. Er is echter zelden sprake van een gegarandeerde continuïteit van de financiering. Dit moet worden afgezet tegen de noodzaak van stabiliteit.

Geef in de onderbouwing van het antwoord op deze Requirement informatie over de volgende onderwerpen:

- De hosting van het digitale archief is – vanwege de stabiliteit en de duurzaamheid op de lange termijn - in handen van een erkende instelling die past bij de Designated Community.
- Het digitale archief heeft voldoende financiële middelen, inclusief personele middelen, IT-middelen en eventueel reisbudgetten, idealiter voor een periode van drie tot vijf jaar.
- Het digitale archief biedt het personeel doorlopende mogelijkheden om opleidingen te volgen en te werken aan professionele ontwikkeling.
- De breedte en diepgang van de expertise van zowel de organisatie als het personeel, inclusief die van netwerken en organen waarvan de organisatie deel uitmaakt (zoals nationale en internationale organen), sluiten aan op de missie.

Bij deze Requirement kan, indien beschikbaar, een uitvoerige beschrijving worden gegeven van de taken van het digitale archief en van de vaardigheden die hiervoor nodig zijn. Die beschrijving is niet verplicht, omdat dit soort details verder strekt dan de reikwijdte van de basiscertificering.

Toegang tot objectief advies van deskundigen, d.w.z. buiten het advies van het eigen personeel, komt aan bod in R6 (Expert guidance).

### Aanvullende toelichting R5.

Geef in de onderbouwing van het antwoord op deze Requirement een beschrijving van de besluitvormingsprocessen van het management van de organisatie en bijbehorende aspecten zoals aantal fte's, kennisniveaus, etc. Ter waarborging van consistente kwaliteitsnormen dienen medewerkers een goede opleiding te hebben op het gebied van databeheer. Het is ook belangrijk dat inzicht wordt gegeven in het aantal medewerkers met een vaste of tijdelijke aanstelling en wat voor mogelijk effect dit zou kunnen hebben op de professionele kwaliteit van het digitale archief, met name voor de preservering van objecten op de lange termijn.

In hoeverre is de financiering structureel of op projectbasis? Kan dit worden uitgedrukt in fte's?

Hoe vaak vindt de periodieke verlenging van de financiering plaats?

# 6. Expert guidance

## R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either in-house, or external, including scientific guidance, if relevant).

(Het digitale archief wint structureel advies en feedback van deskundigen in (zowel intern als extern, bijvoorbeeld wetenschappelijk advies, indien relevant.)

Compliance Level:

### Antwoord

### Toelichting

Een doeltreffend digitaal archief speelt in op ontwikkelingen op het gebied van datatypes, datavolumes en dataverwerkingssnelheden. Daarnaast maakt het gebruik van de meest effectieve nieuwe technologieën om toegevoegde waarde te kunnen blijven bieden aan de Designated Community. De wereld verandert in rap tempo en daarom is het raadzaam dat een digitaal archief zich periodiek verzekert van het advies en de feedback van deskundige gebruikers. Zo blijft het digitale archief relevant en bij de tijd.

Ga in de onderbouwing van het antwoord op deze Requirement in op de volgende vragen:

- Heeft het digitale archief eigen adviseurs of beschikt het over een externe adviescommissie bestaande uit technici, preserveringsdeskundigen, datawetenschappers of vakspecialisten?
- Hoe communiceert het digitale archief met de adviseurs?
- Hoe haalt het digitale archief feedback op bij de Designated Community?

Het antwoord op deze Requirement dient te worden gezien als een bevestiging dat het digitale archief niet alleen toegang heeft tot deskundig advies van het eigen personeel (zie R5: Organizational infrastructure) maar ook tot objectief advies van externe deskundigen.

### Aanvullende toelichting R6.

De reviewers willen bewijs zien dat het digitale archief toegang heeft tot een breder netwerk van deskundigen. Het gaat hierbij om aantoonbare toegang tot advies en begeleiding ten behoeve van zowel de dagelijkse werkzaamheden als het monitoren van mogelijke toekomstige uitdagingen (d.w.z. om voeling te houden met technologische ontwikkelingen en de Designated Community). Als een deel van die informatie al bij 'R0. Brief Description of the Repository's Designated Community' en 'Other relevant information' is gegeven, dan is een verwijzing hier voldoende.

# Beheer van digitale objecten

## 7. Data integrity and authenticity

### R7. The repository guarantees the integrity and authenticity of the data.

(Het digitale archief waarborgt de integriteit en de authenticiteit van de data.)

Compliance Level:

### Antwoord

### Toelichting

Het digitale archief moet aantonen dat het de integriteit en de authenticiteit van de data en metadata waarborgt zowel tijdens de verwerking en opslag van de data als bij de toegang tot die data. Deze Requirement geldt voor de gehele levenscyclus van data in het digitale archief.

Om de integriteit van data en metadata te bewaken, moeten alle bewuste wijzigingen worden vastgelegd. Ook de reden en de initiatiefnemer van elke wijziging dienen te worden vastgelegd. Er dienen maatregelen te zijn getroffen om mogelijk ongewenste of ongeoorloofde wijzigingen op te sporen en de juiste versies van data en metadata te herstellen.

Bij authenticiteit gaat het om de mate van betrouwbaarheid en de herkomst van de oorspronkelijke aangeleverde data. Dan gaat het bijvoorbeeld om de relatie tussen de oorspronkelijke data en de data zoals ze worden uitgeleverd, en om de vraag of de bestaande relaties tussen datasets en/of metadata onderhouden worden.

Neem in de onderbouwing van het antwoord op deze Requirement het volgende op:

- een beschrijving van de controles die worden uitgevoerd om te verifiëren of een digitaal object sinds het depot onveranderd en onbeschadigd is (*fixity*-controles);
- documentatie die aantoont dat de data en metadata compleet zijn;
- informatie over de manier waarop alle wijzigingen in data en metadata worden vastgelegd;
- een beschrijving van het beleid voor versiebeheer;
- bewijs dat relevante internationale standaarden en verdragen worden nageleefd (voeg een lijst van deze standaarden en verdragen bij).

Ga in de onderbouwing van het authenticiteitsbeheer in op de volgende vragen:

- Heeft het digitale archief een beleid voor datawijzigingen? Zijn dataproducenten hiervan op de hoogte?
- Houdt het digitale archief de herkomst van en wijzigingen in data bij?
- Onderhoudt het digitale archief links naar metadata of andere datasets? Zo ja, hoe?
- Vergelijkt het digitale archief de essentiële kenmerken van verschillende versies van een bestand? Hoe?
- Controleert het digitale archief de identiteit van depotgevers?

## Aanvullende toelichting R7.

De reviewers zijn gebaat bij een helder overzicht van alle processen en instrumenten van het digitale archief voor het bewaken van de authenticiteit en de integriteit tijdens de gehele levenscyclus van de curatie, inclusief een beschrijving in hoeverre zaken binnen die levenscyclus al dan niet zijn geautomatiseerd. Verder willen de reviewers weten hoe het digitale archief dergelijke processen, instrumenten en praktijken documenteert. Zoals eerder aangegeven, kan het nuttig zijn om op elk onderdeel hierboven apart te reageren of om integriteit en authenticiteit afzonderlijk toe te lichten, maar maak er wel een lopende tekst van.

Geef in de onderbouwing van het antwoord een beschrijving van de manier waarop wijzigingen in of aan data worden vastgelegd (bijvoorbeeld in een audit trail).

# 8. Appraisal

## R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.

(Het digitale archief accepteert data en metadata op basis van vooraf gedefinieerde criteria, zodat datagebruikers er zeker van kunnen zijn dat die data en metadata relevant en begrijpelijk voor hen zijn.)

Compliance Level:

### Antwoord

### Toelichting

Waardering is van belang om te kunnen beoordelen of de data aan alle selectiecriteria voldoen en goed worden gepreserveerd. Waardering en herwaardering na verloop van tijd zorgen ervoor dat data relevant en begrijpelijk blijven voor de Designated Community.

Ga in de onderbouwing van het antwoord op deze Requirement in op de volgende vragen:

- Gebruikt het digitale archief een ontwikkelbeleid voor de selectie van data/collecties voor archivering?
- Wat is het beleid ten aanzien van data die niet binnen het kader van de missie of collectie vallen?
- Heeft het digitale archief procedures om te bepalen of de benodigde metadata zijn aangeleverd voor het interpreteren of gebruiken van data/collecties?
- Wordt automatisch vastgesteld of metadata aan relevante metadataschema's voldoen?
- Wat is de aanpak ten aanzien van aangeleverde metadata die ontoereikend zijn voor duurzame preservering?
- Heeft het digitale archief een lijst met voorkeursformaten gepubliceerd?
- Zijn er kwaliteitscontroles om ervoor te zorgen dat dataproducenten zich aan de voorkeursformaten houden?
- Wat is het beleid ten aanzien van data die niet in een voorkeursformaat worden aangeleverd?
- Hoe verloopt het verwijderen van objecten in de collectie, waarbij ook rekening moeten worden gehouden met de gevolgen voor bestaande *persistent identifiers*?

In deze Requirement gaat het om selectiecriteria voor het aanleveren van data. De kwaliteit en verrijking van data tijdens het curatieproces komen bij R11 (Data quality) aan bod.

### Aanvullende toelichting R8.

Beschrijf de procedures die ervoor zorgen dat in het digitale archief alleen data worden geaccepteerd die aansluiten bij het collectiebeleid. Voor duurzame preservering van de data en relevant gebruik door de Designated Community moeten medewerkers met alle benodigde informatie en procedures bekend zijn en over de benodigde deskundigheid beschikken.

Wellicht moeten de selectiecriteria na verloop van tijd worden bijgesteld en moeten digitale objecten opnieuw worden gewaardeerd om de collectie relevant en bruikbaar te houden voor de Designated Community, met name vanwege nieuwe technologieën, sociale normen of wetgeving (denk aan databescherming of IE-rechten). Het digitale archief moet beleid en gedocumenteerde procedures hebben voor het verwijderen van objecten uit de collectie.

# 9. Documented storage procedures

## R9. The repository applies documented processes and procedures in managing archival storage of the data.

(Het digitale archief gebruikt gedocumenteerde processen en procedures om de opslag van data te beheren.)

Compliance Level:

### Antwoord

### Toelichting

Digitale archieven moeten data en metadata opslaan vanaf het moment van aanlevering tot aan het moment van gebruik. Dat geldt dus ook tijdens het gehele verwerkingsproces. Archieven met digitale preservering moeten voldoen aan de OAIS-eisen voor 'archiefopslag'.

Ga in de onderbouwing van het antwoord op deze Requirement in op de volgende vragen:

- Hoe zijn de relevante processen en procedures gedocumenteerd en hoe worden ze beheerd?
- Heeft het digitale archief een goed overzicht van alle opslaglocaties? En hoe worden die beheerd?
- Heeft het digitale archief beleid voor het maken van meerdere kopieën? Zo ja, hoe ziet dat beleid eruit?
- Wordt voor dat beleid gebruikgemaakt van risicobeheersing?
- Welke procedures hanteert het digitale archief om ervoor te zorgen dat kopieën identiek zijn?
- Hoe wordt omgegaan met mogelijk verval van opslagmedia? En hoe wordt dit gemonitord?

Gedetailleerde informatie over de technische aspecten van de opslag hoort bij R15 (Technical infrastructure) en specifieke maatregelen voor fysieke en logische beveiliging bij R16 (Security).

### Aanvullende toelichting R9.

De reviewers willen weten (1) welke opslaglocaties worden gebruikt ter ondersteuning van de curatieprocessen, (2) hoe data in elke omgeving worden beheerd, en (3) hoe wijzigingen in opslagdocumentatie worden gemonitord en beheerd. Belangrijk is dat procedures zodanig zijn vastgelegd en gestandaardiseerd dat verschillende databeheerders onafhankelijk van elkaar tot grotendeels hetzelfde resultaat komen. Voorbeelden van bewijsmateriaal zijn stroomdiagrammen met informatie over aanlevering, preservering en toegangslocaties (en mogelijke toegangsbeperkingen). Bewijsmateriaal voor archiefopslag zou kunnen bestaan uit beschrijvingen van de manier waarop de opslag in meerdere locaties is geregeld (on-site, near-site, off-site), van de mix aan opslagmedia en van eventuele redundantie (zoals een beschrijving van het waarborgen van de integriteit door middel van checksums).

# 10. Preservation plan

## R10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

(Het digitale archief neemt verantwoordelijkheid voor duurzame preservering en doet dit op een gestructureerde en goed gedocumenteerde manier.)

Compliance Level:

### Antwoord

### Toelichting

Het digitale archief, de depotgevers van de data en de Designated Community moeten inzicht hebben in de verantwoordelijkheden die het preserveringsniveau van elk aangeleverd object in het digitale archief met zich meebrengt. Het digitale archief moet bevoegd zijn om die verantwoordelijkheden op zich te nemen. Er moeten gedocumenteerde procedures zijn en garanties dat die procedures ook worden uitgevoerd.

Ga in de onderbouwing van het antwoord op deze Requirement in op de volgende vragen:

- Heeft het digitale archief een gedocumenteerd preserveringsbeleid?
- Begrijpen alle partijen de aard van de verantwoordelijkheid voor de preservering van elk object? Hoe is dit gedefinieerd?
- Liggen er plannen voor migraties of soortgelijke maatregelen in het geval van veroudering van data?
- Voorziet de overeenkomst tussen de depotgever en het digitale archief in alle noodzakelijke activiteiten om aan de verantwoordelijkheden te voldoen?
- Is de overdracht van beheer en verantwoordelijkheid duidelijk voor zowel de depotgever als het digitale archief?
- Is het digitale archief bevoegd om objecten te kopiëren, te wijzigen, op te slaan en toegankelijk te maken?
- Is er goede documentatie over preserveringsactiviteiten? Denk hierbij aan de overdracht van beheer en standaarden voor aanlevering en archivering.
- Zijn er maatregelen getroffen om ervoor te zorgen dat die activiteiten ook worden uitgevoerd?

De bevoegdheden omtrent de toegang tot en het gebruik van data en het monitoren van de naleving van die bevoegdheden moeten in R2 (Licenses) worden beschreven.

### Aanvullende toelichting R10.

Een preserveringsplan (digitale duurzaamheidsbeleidsplan) is een gedocumenteerde aanpak voor het definiëren en uitvoeren van preserveringsactiviteiten. In de Requirements wordt geen onderscheid gemaakt tussen een preserveringbeleid, -plan, -strategie of -actieplan.

Voorzie de reviewers van duidelijke, goed beheerde documentatie die garanties biedt voor: (1) een gestructureerde aanpak van de preservering voor de lange termijn, (2) duurzame toegang tot datatypes, ook bij formaatwijzigingen, en (3) voldoende documentatie ten behoeve van de bruikbaarheid door de Designated Community. Geef in het antwoord op de Requirement aan of het digitale archief preserveringsniveaus heeft gedefinieerd en, zo ja, hoe deze worden toegepast. Het preserveringsplan moet zodanig worden beheerd dat tijdig en op een stabiele manier wordt ingespeeld op veranderingen in de datatechnologie of de behoeften van gebruikers.

Zijn er verschillen tussen de preserveringsniveaus van bepaalde soorten objecten of collecties? Leg dan uit wat de verschillen in het preserveringsbeleid zijn en welke criteria worden toegepast om het preserveringsniveau te bepalen. Dat kan bijvoorbeeld relevant zijn als de bestandsgrootte van een bepaald object of als de gevoeligheid van de desbetreffende data bepaalt hoeveel redundante kopieën er worden gemaakt, of wanneer alleen in voorkeursformaten aangeleverde objecten naar standaard preserveringsformaten worden geconverteerd en in de toekomst worden gemigreerd.

Staat in het antwoord geen link naar een gedocumenteerd preserveringsbeleid, dan kan het Compliance Level niet hoger zijn dan 3. Bovendien dient er voor de volgende review wel zo'n gedocumenteerd preserveringsbeleid beschikbaar te zijn.

# 11. Data quality

## R11. The repository has appropriate expertise to address technical data and metadata quality and ensures that sufficient information is available for end users to make quality-related evaluations.

(Het digitale archief heeft voldoende deskundigheid in huis om de kwaliteit van de technische data en metadata te garanderen en zorgt ervoor dat eindgebruikers over voldoende informatie beschikken om die kwaliteit te beoordelen.)

Compliance Level:

### Antwoord

### Toelichting

Digitale archieven moeten ervoor zorgen dat de Designated Community over voldoende informatie beschikt om de kwaliteit van de data te beoordelen. Hoe meer multidisciplinair de Designated Community is, hoe relevanter die kwaliteitsbeoordeling. Gebruikers hebben dan immers misschien zelf niet voldoende ervaring om op basis van de data een kwaliteitsanalyse te maken. Digitale archieven moeten in staat zijn om de volledigheid en kwaliteit van de data en metadata te beoordelen.

Bepaalde tekortkomingen in de kwaliteit van data, of bijbehorende metadata, kunnen relevant zijn vanwege hun onderzoekswaarde, maar dit betekent niet dat een gebruiker er geen gebruik van kan maken. Die kan op basis van de bijgeleverde documentatie zelf bepalen of ze bruikbaar zijn.

Geef voor deze Requirement een beschrijving van:

- het beleid ten aanzien van de kwaliteit van de data en metadata;
- de kwaliteitscontroles voor het waarborgen van de volledigheid en begrijpelijkheid van de aangeleverde data. Neem verwijzingen op naar kwaliteitsstandaarden en rapportagemechanismen die relevant zijn voor de doelgroep en beschrijf hoe eventuele problemen worden opgelost (worden foutieve data bijvoorbeeld ter correctie teruggestuurd naar de depotgever, worden ze door het digitale archief zelf rechtgezet, worden ze op een of andere manier gemarkeerd, of wordt het probleem vermeld in de bijbehorende metadata?);
- de opties die de Designated Community heeft om commentaar te geven of om data en metadata te beoordelen;
- mogelijke verwijzingen naar gerelateerde bronnen of links met citatie-indexen.

In deze Requirement gaat het om kwaliteitsstandaarden en kwaliteitsborging tijdens de curatie. Selectiecriteria komen aan bod in R8 (Appraisal).

### Aanvullende toelichting R11.

Maak in het antwoord duidelijk dat het digitale archief ervan doordrongen is welke kwaliteitsniveaus redelijkerwijs van depotgevers kunnen worden verwacht. Zorg ervoor dat uit de onderbouwing blijkt hoe kwaliteit tijdens het preserveringsproces wordt geborgd. Beschrijf ook welke verwachtingen de Designated Community heeft ten aanzien van kwaliteit. Van zowel het digitale archief als de depotgevers wordt verwacht dat elk mogelijk aspect van data of metadata dat niet aan de verwachte standaard voldoet, goed wordt gedocumenteerd.

# 12. Workflows

## R12. Archiving takes place according to defined workflows from ingest to dissemination.

(Bij de archivering wordt gebruikgemaakt van gedefinieerde workflows vanaf het moment van opname van data tot en met de verspreiding ervan.)

Compliance Level:

### Antwoord

### Toelichting

Er moeten workflows zijn gedefinieerd en gedocumenteerd op basis van de activiteiten van het digitale archief. Dit is noodzakelijk voor de consistentie van het gebruik van de datasets en de bijbehorende dienstverlening en om te voorkomen dat bepaalde handelingen ad hoc worden verricht. Ook moeten er maatregelen zijn getroffen voor het managen van wijzigingen. Voor het specificeren van de workflowfuncties kan gebruik worden gemaakt van het OAIS-referentiemodel.

Geef in de onderbouwing van het antwoord op deze Requirement een beschrijving van:

- de workflows en bedrijfsprocessen;
- de communicatie met depotgevers en gebruikers over het gebruik van data;
- de veiligheidsniveaus en de gevolgen voor workflows (bijv. bescherming privacy);
- de kwalitatieve en kwantitatieve controle van output;
- de datatypes die worden beheerd en alle mogelijke gevolgen voor de workflows;
- de besluitvorming binnen de workflows (bijv. bij wijziging van data via migratie of conversie).
- het veranderingsbeheer van workflows.

Het doel van deze Requirement is te laten zien dat alle workflows zijn gedocumenteerd.

### Aanvullende toelichting R12.

Voorzie de reviewers van bewijsmateriaal dat alle activiteiten in alle processen op een consistente, nauwgezette en goed gedocumenteerde manier worden beheerd en dat alle mogelijke wijzigingen in die processen correct worden uitgevoerd, geëvalueerd, opgeslagen en beheerd.

Voor deze Requirement is het niet nodig om uitvoerige beschrijvingen van workflows te geven. Maak wel inzichtelijk hoe en waar deze workflows zijn gedocumenteerd.

# 13. Data discovery and identification

## R13. The repository enables users to discover the data and refer to them in a persistent way through proper citation.

(Het digitale archief stelt gebruikers in staat de data in het archief te ontsluiten en er altijd met correcte citaties naar te verwijzen.)

Compliance Level:

### Response

### Guidance

Om data te kunnen delen, moet je ze op een doeltreffende manier kunnen vinden en ontsluiten. En op het moment dat ze ontsloten zijn, moet je er goed naar kunnen verwijzen, onder andere met persistent identifiers die ervoor zorgen dat de data ook in de toekomst toegankelijk zijn.

Ga in de onderbouwing van het antwoord op deze Requirement in op de volgende vragen:

- Heeft het digitale archief zoekfuncties?
- Heeft het digitale archief een doorzoekbare catalogus van metadata die aan relevante internationale standaarden voldoet?
- Welke 'persistent identifiers' gebruikt het digitale archief?
- Biedt het digitale archief de mogelijkheid voor het geautomatiseerd verkrijgen van metadata?
- Is het digitale archief opgenomen in een of meer specifieke of generieke bronnenregisters?
- Doet het digitale archief aanbevelingen voor datacitaties?

### Aanvullende toelichting R13.

Toon in de onderbouwing met bewijs aan dat de preservering van data en metadata bevorderlijk is voor het vinden en ontsluiten van duidelijk gedefinieerde en geïdentificeerde digitale objecten. Toon ook aan dat gebruikers in staat worden gesteld om conform domeinspecifieke standaarden koppelingen met gerelateerde digitale objecten te maken. Voor de Designated Community moet duidelijk zijn hoe data worden geciteerd, zodat individuen en organisaties die een bijdrage hebben geleverd aan het maken van die data, op een correcte manier worden aangehaald en dat data aan hen worden toegeschreven.

# 14. Data reuse

## R14. The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.

(Het digitale archief maakt hergebruik van data voor de lange termijn mogelijk en zorgt ervoor dat de juiste metadata beschikbaar zijn voor goed begrip en gebruik van die data.)

Compliance Level:

### Antwoord

### Toelichting

Digitale archieven moeten ervoor zorgen dat data altijd begrijpelijk zijn en ook in de toekomst op een doeltreffende manier kunnen worden gebruikt, ook als er iets verandert in de technologie of de basiskennis van de Designated Community. Het doel van deze Requirement is om te bepalen of de getroffen maatregelen afdoende zijn om hergebruik van data te waarborgen.

Ga in de onderbouwing van het antwoord op deze Requirement in op de volgende vragen:

- Welke metadata geeft het digitale archief op het moment dat data worden opgevraagd?
- Hoe zorgt het digitale archief ervoor dat de data altijd begrijpelijk blijven?
- Worden de data weergegeven in formaten die de Designated Community ook gebruikt? Zo ja, welke formaten zijn dat?
- Zijn er maatregelen getroffen om rekening te houden met mogelijke formaatwijzigingen?

Het concept ‘hergebruik’ is van cruciaal belang als naast de primaire data ook de output van secundaire analyses in een digitaal archief wordt gedeponeerd. In zo’n geval kan het steeds moeilijker worden om de herkomstketen van data en mogelijke rechtenkwesties helder te houden.

### Aanvullende toelichting R14.

Maak in het antwoord op deze Requirement duidelijk dat er bij het digitale archief voldoende kennis aanwezig is over vormen van hergebruik en over de behoeften van de Designated Community wat betreft gangbare praktijken, technische omgeving en (de naleving van) relevante standaarden. Veranderingen in de technologie en in de door de Designated Community gebruikte methodieken en normen kunnen betekenen dat het nodig is om nog eens goed na te denken over het formaat waarin de data worden verspreid. Ook relevante hoogwaardige metadata die voldoen aan een generieke en/of domeinspecifieke standaard spelen een belangrijke rol. Neem dit ook mee in de onderbouwing, want het is van groot belang voor het ontwerpen van curatieprocessen die ervoor zorgen dat digitale objecten ook in de toekomst begrijpelijk en bruikbaar blijven voor de Designated Community. Gebruikt het digitale archief alleen een generieke metadatastandaard (zoals Dublin Core of DataCite)? Maak dan in de onderbouwing duidelijk dat hiermee gewaarborgd is dat de gepreserveerde content ook in de toekomst begrijpelijk blijft voor de Designated Community.

# Technologie

## 15. Technical infrastructure

**R15. The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.**

(Het digitale archief werkt met goed ondersteunde besturingssystemen en andere belangrijke infrastructurele software en maakt gebruik van hardware- en softwaretechnologieën die geschikt zijn voor de dienstverlening aan de Designated Community.)

Compliance Level:

### Antwoord

### Toelichting

Voor beschikbaarheid van de dienstverlening moeten digitale archieven over betrouwbare, stabiele infrastructuren beschikken. De hardware en software moeten relevant en geschikt zijn voor de Designated Community en voor de functies van het digitale archief. Het OAIS-referentiemodel bevat een beschrijving van de functies waaraan een digitaal archief moet voldoen om tegemoet te komen aan de eisen van de gebruikers.

Ga in de onderbouwing van het antwoord op deze Requirement in op de volgende vragen:

- Welke referentiestandaarden gebruikt het digitale archief? Zijn het internationale en/of domeinspecifieke standaarden? Hoe vaak worden die gecontroleerd?
- Hoe zijn de standaarden geïmplementeerd? Wordt er op belangrijke onderdelen van de standaard afgeweken? Zo ja, geef een toelichting.
- Heeft het digitale archief beleid voor infrastructuurontwikkeling? Zo ja, hoe ziet dat beleid eruit?
- Houdt het digitale archief een softwarecatalogus bij en beschikt het over systeemdocumentatie?
- Gebruikt het digitale archief door gebruikers ondersteunde software? Zo ja, geef hiervan een beschrijving.
- Zijn de beschikbaarheid, bandbreedte en connectiviteit toereikend om aan de behoeften van de Designated Community te voldoen?
- Heeft het digitale archief een rampenplan en een continuïteitsplan? Zijn er met name procedures en regelingen voor snel herstel en backups van essentiële diensten in geval van storingen? Hoe zien die eruit?

De bestuurlijke aspecten van de bedrijfscontinuïteit, het rampenplan en het continuïteitsplan komen aan bod bij R3 (Continuity of Access). Informatie over het opslagproces dient te worden gegeven bij R9 (Documented storage procedures). Beveiliging komt aan bod bij R16 (Security).

### Aanvullende toelichting Guidance R15.

De workflows en de mensen die de dienstverlening van het digitale archief verzorgen, moeten worden ondersteund door een adequate technologische infrastructuur die aansluit op de behoeften van de Designated Community en die het digitale archief in staat stelt kortstondige rampen het hoofd te bieden. De reviewers willen bewijs zien dat de aanvrager inzicht heeft in het bredere ecosysteem van de standaarden, instrumenten en technologieën voor het beheer en de curatie van (onderzoeks)data en dat de gekozen opties aansluiten bij

de specifieke eisen van het digitale archief. Dit zou, indien mogelijk, moeten worden aangetoond met behulp van een referentiemodel.

Voorbeelden van relevante standaarden zijn SDI-standaarden (Spatial Data Infrastructure), Open Geospatial Consortium (OGC), W3C en ISO-normen.

Zijn er voor real-time tot bijna real-time datastromen 24/7-verbindingen met publieke en private netwerken met een bandbreedte die toereikend is voor de wereldwijde en/of regionale verantwoordelijkheden van het digitale archief?

# 16. Security

## R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.

(De technische infrastructuur van het digitale archief is zodanig dat zowel de faciliteit zelf als de data, producten, diensten en gebruikers zijn beschermd.)

Compliance Level:

### Antwoord

### Toelichting

Het digitale archief heeft mogelijke bedreigingen in kaart gebracht, risico's bepaald en voor een consistent beveiligingssysteem gezorgd. Er moet een beschrijving zijn van de scenario's die het digitale archief hanteert in geval van kwaadwillige handelingen, menselijke fouten of technische storingen die een bedreiging vormen voor het digitale archief zelf of voor de data, producten, diensten of gebruikers. Het digitale archief bepaalt hoe waarschijnlijk dergelijke scenario's zijn, hoe groot de impact ervan is, welke risiconiveaus acceptabel zijn en welke maatregelen moeten worden getroffen om de bedreigingen voor het digitale archief en de Designated Community af te wenden. Dit dient een doorlopend proces te zijn.

Geef voor deze Requirement een beschrijving van:

- het IT-beveiligingssysteem, de medewerkers die op een of andere manier betrokken zijn bij de beveiliging (bijv. beveiligingsmedewerkers) en de instrumenten voor risicoanalyse (bijv. DRAMBORA[3]);
- de vereiste beveiligingsniveaus en hoe die worden ondersteund;
- eventuele authenticatie- en autorisatieprocedures voor veilig beheer van de toegang tot de gebruikte systemen (bijv. Shibboleth, OpenAthens).

De opslagprocessen en technische infrastructuur waarvoor deze beveiligingsmaatregelen gelden, dienen bij respectievelijk R9 (Documented storage procedures) en R15 (Technical Infrastructure) te worden beschreven.

### Aanvullende toelichting R16.

De reviewers willen bewijs zien dat de aanvrager begrijpt welke technische risico's verbonden zijn aan zowel de fysieke omgeving als de dienstverlening aan de Designated Community. Toon daarom aan welke voorzieningen zijn getroffen om beveiligingsincidenten te voorkomen, op te sporen en te bestrijden.

Hoe houdt het digitale archief, de hostingpartner of de externe dienstverlener greep op de beveiliging van de technische infrastructuur? Wie is hiervoor verantwoordelijk?

Zijn de authenticatie- en autorisatieprocedures toereikend voor het waarborgen van de beveiliging van de data in het digitale archief tijdens alle stappen van de workflow (bijv. met tweetraps-authenticatie voor gevoelige data)?

Wat is het algemene beleid voor de beveiliging van alle systemen? Denk hierbij aan onder andere netwerkbeveiliging, detectie van ongeautoriseerde toegang, fysieke beveiliging van de faciliteit en wachtwoordbeleid.

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

## Feedback aanvrager

# Opmerkingen/feedback

Deze Requirements dienen niet als statisch te worden beschouwd. We staan open voor input en ideeën waarmee we de certificeringsprocedure van CoreTrustSeal kunnen verbeteren. In toekomstige versies nemen we uw opmerkingen en bijdragen over de kwaliteit en relevantie van de Requirements graag mee.

### Antwoord