CERTIFICERINGSSCHEMA EDUKOPPELING

DATUM	27 oktober 2014
VERSIE	1.1
AUTEUR	Kennisnet
LICENTIE	Creative Commons Naamsvermelding

INHOUDSOPGAVE

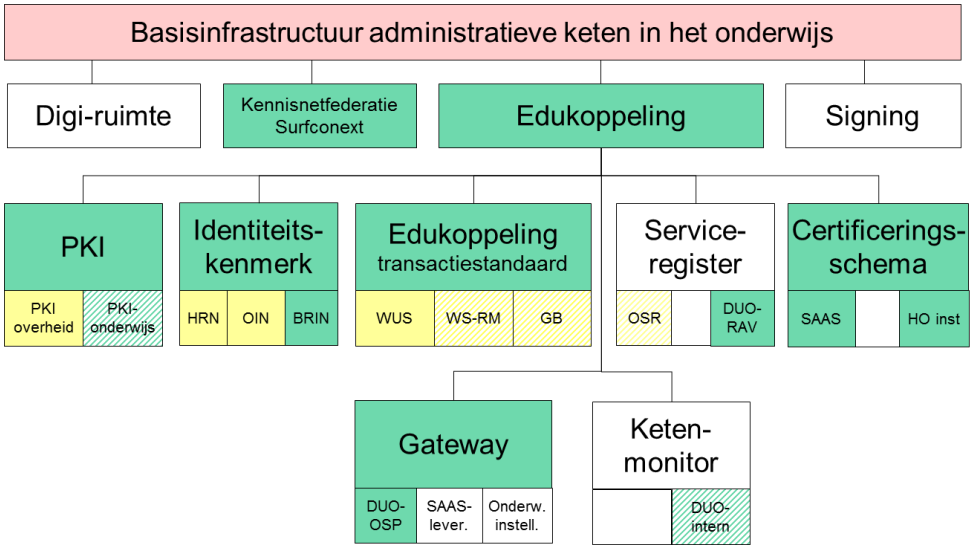
1 INLEIDING

1.1 Achtergrond en aanleiding

Het Samenwerkingsplatform Informatie Onderwijs (SION) is een samenwerkingsverband van de zes onderwijsraden (PO-raad, VO-raad, MBO-raad, AOC-raad, Vereniging Hoge scholen en VSNU) die zich bezighouden met het verbeteren van de informatiehuishouding voor wat betreft de gemeenschappelijke vraagstukken die de verschillende deelsectoren in het onderwijs overstijgen. Een van de vraagstukken behelst een veilige en uniforme manier van gegevensuitwisseling binnen de administratieve keten in het onderwijsdomein.

Alle ketenpartijen moeten erop kunnen vertrouwen dat gegevens die aan elkaar worden geleverd via leveranciers van clouddiensten op de juiste manier worden verwerkt. De cloudleverancier zal, via bijvoorbeeld het uitvoeren van onafhankelijke audits, aan alle ketenpartijen moeten kunnen aantonen dat dat vertrouwen gerechtvaardigd is. Met dit schema kunnen binnen het onderwijsdomein daarom clouddiensten en -leveranciers worden getoetst op basis van een gezamenlijk opgesteld 'normenkader'.

Deze standaard voor audit en assurance, die voldoet aan de benodigde beveiligingsnormen, is tot stand gekomen met diverse ketenpartijen, waaronder Kennisnet, OCW/DUO en leveranciers. De standaard is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA[1]) en wordt hierbinnen geschaard bij andere ICT-infrastructurele afspraken en voorzieningen onder de noemer Edukoppeling (figuur 1).



Figuur 1: Edukoppeling (Geel = Gerealiseerd, niet onderwijsspecifiek, Groen = Gerealiseerd, onderwijsspecifiek, Wit = Nog in ontwikkeling)

[1] http://www.wikixl.nl/wiki/rosa

1.2 Doel

Het Certificeringsschema Edukoppeling is bedoeld voor leveranciers van clouddiensten.
Het doel van het certificeringsproces is om vertrouwen te creëren in de betrouwbaarheid van de door de leveranciers geleverde clouddiensten.

Dit certificeringsschema:

1. specificeert de minimale basisset (de geselecteerde basisset aan controls[2] uit de Cloud Control Matrix van de Cloud Security Alliance) waaraan een toepassing moet voldoen om te mogen worden ingezet voor clouddiensten; en
2. beschrijft de wijze waarop wordt vastgesteld of aan deze basisset wordt voldaan.

Een cloudleverancier moet aan de normen in dit schema voldoen, vóórdat de betreffende cloud-dienst binnen de context van Edukoppeling mag worden ingezet.

1.3 Scope

De huidige scope van het certificeringsschema is gericht op het ketenproces aanmelden, waarbij gegevens via DUO hergebruikt kunnen worden in een digitaal aanmeldformulier. Het certificeringsschema is momenteel alleen bedoeld voor de leveranciers van clouddiensten waaraan DUO gegevens levert.

De scope van het schema wordt de komende jaren uitgebreid naar andere gegevenslevering vanuit DUO in het kader van bekostiging (Doorontwikkelen Bron) en toetsen/examineren (Facet).

1.4 Samenhang met andere initiatieven

Binnen het samenwerkingsplatform wordt gewerkt aan een ROSA katern privacy en beveiliging, waarin kaders (principes) opgenomen worden waar ketenpartijen, dus ook scholen, (op termijn) aan dienen te voldoen. Voor het hoger onderwijs zijn door SURF juridische normenkaders ontwikkeld voor zowel leveranciers van clouddiensten. Vanuit de ROSA wordt gewerkt aan afstemming en samenhang tussen het schema en andere initiatieven binnen en buiten het onderwijs. In bijlage E is een lijst opgenomen met veelgestelde vragen over de samenhang van dit schema met andere initiatieven.

1.5 Governance

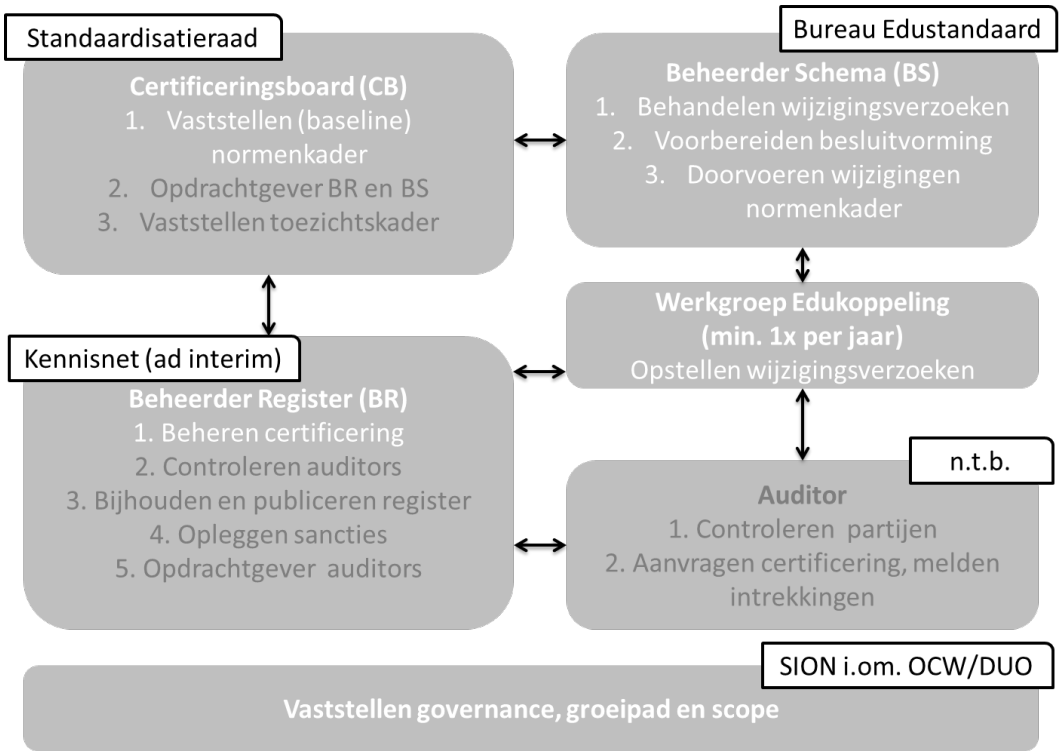
Het eigenaarschap van dit certificeringsschema ligt momenteel binnen SION. Het is de verantwoordelijkheid van Kennisnet als uitvoerder van het programma om, gedurende de looptijd van het programma (tot eind 2015), te zorgen voor de certificering van leveranciers en de registratie hiervan. Vooralsnog wordt deze rol aangeduid als Beheerder Register.

---

[2] In dit document worden de begrrippen ‘controls’ en ‘normen’ door elkaar gebruikt, de betekenis is echter dezelfde

Binnen SION wordt in overleg met OCW/DUO de scope van het schema bepaald (zie par. 1.3), evenals de wijze waarop wordt vastgesteld of aan de basisset met controls is voldaan (zie par. 1.6).
Het beheer van de minimale basisset met controls in het certificeringsschema Edukoppeling wordt belegd bij bureau Edustandaard, die ook andere afspraken binnen het onderwijsdomein beheert. Bureau Edustandaard ziet dus alleen toe op de inhoudelijke wijzigingen van de basisset. Vooralsnog wordt deze rol aangeduid als Beheerder Schema.

In een open werkgroep binnen Edustandaard wordt een jaarlijkse evaluatie verzorgd om na te gaan in hoeverre aan de basisset voldaan kan en moet worden (compliance eis) en of de minimale basisset met controls uitgebreid dient te worden (zie par. 4.3). Het vaststellen van deze basisset geschied dus door de Standaardisatieraad in de rol van Certificeringsboard.



Figuur 2: Governance Certificeringsschema Edukoppeling

(witte tekst = belegd, grijze tekst = nog niet belegd)

1.6 Groeipad

Op dit moment wordt er nog gecertificeerd op basis van een zelfverklaring. In de toekomst zal dit uitgroeien naar externe audits. Het tempo hiervoor wordt binnen SION in overleg met OCW/DUO bepaald. Zodra ook de rol van Eigenaar en de rol van Beheerder Register duurzaam is belegd dient ook het onderdeel sanctieregime verder uitgewerkt te worden (zie par 4.2).

2 WAAR MOET IK AAN VOLDOEN?

2.1 Bron voor normen

Cloud dienstverlening is een zodanig nieuw en veelomvattend type dienstverlening dat er nog geen wereldwijd geaccepteerde set aan betrouwbaarheidseisen bestaat. Tegelijkertijd zijn er wel initiatieven (zoals de Cloud Security Alliance en Eurocloud) en vanuit andere belangenorganisaties (bijvoorbeeld ISACA of lokale overheden) om te komen tot een gemeenschappelijke standaard.

Op het moment van de initiële totstandkoming van dit schema (Q4 2013) heeft de Cloud Security Alliance (CSA[3]) een grote voorsprong op andere initiatieven. Dit is onder andere zichtbaar in de uitwerking van een normenkader voor Cloud dienstverlening, de 'Cloud Control Matrix'[4].

Versie 3.0.1 van de Cloud control matrix is daarom als basis gekozen voor de in dit schema opgenomen normen.

2.2 Verantwoording voor selectie van normen

De Cloud Control Matrix (CCM) bestaat uit meer dan 130 normen of controls, verdeeld over 16 domeinen. Op basis van de specifieke functionaliteit van Edukoppeling en het specifieke risicoprofiel, is de keuze gemaakt om uit de volledige set aan controls een minimale basisset te selecteren. De selectie van de controls heeft plaatsgevonden op basis van 3 criteria:

1. Negen aspectgebieden die door CSA worden onderkend als meest cruciale dreigingen voor een veilige cloud waartegen effectieve controls moeten worden ingezet:
   a. Data Breaches
   b. Data Loss
   c. Account or Service Hijacking
   d. Insecure Interfaces and API's
   e. Denial of Service
   f. Malicious Insiders
   g. Abuse of Cloud Services
   h. Insufficient Due Diligence
   i. Shared Technology Vulnerabilities

De CSA heeft zelf een relatie gelegd tussen deze negen aspectgebieden en de controls die een effectieve bescherming vormen tegen deze dreigingen.

2. De samenwerkingspartners rondom Edukoppeling hebben daarnaast drie specifieke risicogebieden geïdentificeerd: interoperabiliteit, betrouwbaarheid en privacy. Er zijn hierbinnen

[3] https://cloudsecurityalliance.org/

[4] https://cloudsecurityalliance.org/research/ccm/

vijf aspectgebieden die specifiek in de context van Edukoppeling aanvullend en specifiek als risicogebied worden gezien:

a. Interoperabiliteit:
    i. de services waarmee gegevens met andere ketenpartijen worden uitgewisseld moeten voldoen aan de Edukoppeling transactie-standaard;
b. Betrouwbaarheid
    i. misbruik door eigen (oud-) medewerkers die toegang kunnen hebben tot de gegevens van de school;
    ii. vermenging van gegevens met die van andere klanten;
    iii. leverancier moet een log of audittrail vastleggen per klantomgeving om het uitvoeren van digitaal (forensisch) onderzoek en audits te ondersteunen;
c. Privacy
    i. tussen cloudleverancier en de onderwijsinstelling moet een bewerkersovereenkomst (zie Bijlage B) worden afgesloten.

Voor deze aspecten heeft de toenmalige Beheerder Register (Kennisnet) een relatie gelegd met de controls die een effectieve bescherming vormen tegen deze dreigingen. Op deze manier zijn enkele de volgende controls aan het nomenkader toegevoegd:

- Daar waar partijen kiezen voor een gegevensuitwisseling conform Edukoppeling moet de thans geldende versie van de transactiestandaard[5] zijn toegepast (AIS-01.a)
- Er is een passende bewerkersovereenkomst afgesloten, conform het geldende model (AAC-03a)
- Persoonsgegevens mogen door de leverancier op geen enkele wijze aan derden ter beschikking worden gesteld (AAC-03b)
- De leverancier geeft volledige transparantie over de locatie van de data door aan te geven in welke plaats(en) / land(en) de data zich bevindt (STA-05a)

3. Tenslotte is er in het kader van een jaarlijkse evaluatie in het voorjaar van 2014 een processpecifieke risico analyse uitgevoerd, waarbij is geïnventariseerd welke risico's (niet alleen cloud specifieke risico's) aandacht verdienen rondom het ketenproces digitaal aanmelden en inschrijven. Deze risico-analyse is in workshopverband met DUO, Kennisnet, instellingen en een leverancier uitgevoerd en bestond uit de volgende stappen:
    a. Toelichting van het proces aanmelden en inschrijven.
    b. Het per processtap inventariseren van de risico's en het benoemen van de entiteit(en) die moet worden geacht het risico te mitigeren.
    c. Het specifiek identificeren van de risico's die bij de cloud leverancier lagen.
    d. Het matchen van deze risico's met de normen in het bestaande certificeringsschema.

[5] http://www.edustandaard.nl/afspraken-en-architectuur/beheerde-afspraken/edukoppeling/

3 HOE VOLDOE IK AAN DE NORMEN?

3.1 Certificeringsproces

Het certificeringsproces valt uiteen in twee onderdelen:

- Het vaststellen van de betrouwbaarheid van de geboden dienstverlening ten aanzien van de vastgestelde normen. Dit betreft de basisset van normen die door de markt als toonaangevend worden beschouwd, aangevuld met specifieke aanvullingen of interpretaties voor Edukoppeling (zie par. 2.2).
- Een beschrijving van de wijze waarop wordt vastgesteld dat de dienstverlening daadwerkelijk voldoet aan de gestelde normen. In deze versie van het schema is gekozen voor de systematiek van een zogenaamde 'zelfverklaring', waarbij de leverancier zelf vaststelt en verklaart dat zijn product of dienst aan de normen voldoet (en in welke mate).

3.2 Interpretation notes

Bij de toepassing van de Control Matrix kan het voorkomen dat onduidelijkheden bestaan over het begrijpen van de norm in relatie tot de specifieke context van Edukoppeling. In die gevallen waar het noodzakelijk is om een specifieke aanvulling of toelichting te geven worden door de schemabeheerder 'interpretation notes' aan de normbeschrijving toegevoegd.

Hierbij wordt er bewust voor gekozen om restrictief te zijn in de aanvullingen, omdat er bij veel aanvullingen op de marktstandaard via een omweg een nieuwe markststandaard wordt gecreëerd.

3.3 Verantwoordelijkheid van de cloudleveranciers

De cloudleveranciers worden geacht om de volgende activiteiten uit te voeren:

1. Kennis nemen van de van toepassing zijnde normen en interpretation notes (zie Bijlage A).
2. Voor zichzelf te bepalen in welke mate aan de betreffende normen en interpretation notes wordt voldaan.
3. Voor zichzelf vast te stellen op welke wijze kan worden aangetoond dat aan de betreffende normen en interpretation notes wordt voldaan. Het wordt geadviseerd de bewijsvoering hiertoe vast te leggen, dit in verband met eventuele latere vragen om openheid van zaken te geven.
4. De mate waarin wordt voldaan vast te leggen in de verplichte bijlage van de Management Letter (zie Bijlage D).
5. Daar waar verbeterpotentieel aanwezig is deze expliciet te benoemen in de bijlage, aangevuld met een planning wanneer leverancier verwacht de verbetering te hebben gerealiseerd. Hierbij kan worden volstaan met een indicatieve planning per kwartaal (bijvoorbeeld 'Q1' of 'Q2').
6. Een zelfverklaring op te stellen, die overeenkomt met de tekst zoals deze in Bijlage C is opgenomen.

3.4 Eisen aan de zelfverklaring

De tekst van de zelfverklaring moet overeenkomen met de tekst zoals deze in Bijlage C is opgenomen. Let op: afwijkingen in de tekst kunnen zonder voorafgaande toestemming van de Beheerder van het register niet worden geaccepteerd.

Een zelfverklaring moet altijd vergezeld gaan van een bijlage waarin wordt aangegeven of en in welke mate aan normen wordt voldaan (zie Bijlage D).

De zelfverklaring is een fysiek document en moet worden ondertekend door een bij de KvK geregistreerde tekenbevoegde.

De zelfverklaring wordt zowel elektronisch als fysiek overhandigt aan de Beheerder Register. De contactgegevens zijn: info@sionderwijs.nl en Paletsingel 32, 2718 NT Zoetermeer.

3.4.1 Periode van geldigheid van de zelfverklaring

De zelfverklaring is maximaal één jaar geldig en dient jaarlijks te worden verstrekt. De zelfverklaring moet jaarlijks op de laatste werkdag vóór 31 januari worden verstrekt.

4 VOLDOE IK AAN DE NORMEN?

4.1 Steekproefsgewijze toetsing

De Beheerder Register heeft het recht om de cloudleveranciers steekproefsgewijs te vragen aantoonbaar te maken dat feitelijk aan de betreffende normen is voldaan. Ook bij gerede twijfel heeft de beheerder het recht om dit te vragen. Hiertoe wordt door de schemabeheerder een onafhankelijke onderzoeker aangesteld die zal beoordelen of de cloudleverancier daadwerkelijk aan de normen voldoet.

De cloudleverancier is verplicht om binnen vier weken aan dit verzoek gehoor te geven en toegang te verlenen aan onderzoekers die door de schemabeheerder worden aangewezen. De tijd en middelen die de cloudleverancier hiervoor moet inzetten kunnen niet worden doorbelast aan de toezichthouder.

4.2 Sancties

Het niet of niet tijdig overleggen van de zelfverklaring kan leiden tot passende sancties.

Mocht gaandeweg een steekproefsgewijze toetsing blijken dat de feitelijke stand van zaken niet overeenstemt met de zelfverklaring en dat aannemelijk is dat de betreffende cloudleverancier dit had kunnen weten kan dit leiden tot passende sancties.

In deze fase is er (nog) geen behoefte om het sanctieregime verder uit te werken. Partijen zullen onderling moeten vaststellen wat een passende sanctie is. De Beheerder Register heeft hierbij de rol van liaison / intermediair.

4.3 Periodieke evaluatie

De Beheerder Schema bespreekt periodiek (minimaal eenmaal per jaar) de opzet en de werking van het certificeringsschema met alle relevante stakeholders, waaronder minimaal: DUO, SURF, saMBO-ICT, Kennisnet en leveranciers van clouddiensten. Tijdens deze evaluatie wordt ook aandacht gegeven aan welke controls in aanmerking moeten/kunnen komen voor gedeeltelijke of volledige compliance. In eerste instantie wordt uitgegaan van een evaluatiefrequentie van eenmaal per jaar.

A Inhoudelijke normen en interpretation notes

De gedachte achter de zelfverklaring is dat de leverancier transparant is over de mate waarin aan de eisen wordt voldaan. Het gaat dus (nog) niet om een onafhankelijke toetsing, waarin deze vaststelling door een derde plaatsvindt. De leverancier dient daarom voor zichzelf te bepalen hoe hij een bepaalde control voor de eigen dienstverlening zou moeten toepassen.

De formuleringen in kolommen 'Control Domain', 'Control ID' en 'Control Specification' zijn overgenomen uit de Cloud Security Agency (CSA) Cloud Control Matrix (CCM) versie 3.0.1. De controls waarvan het 'control id' eindigt op een a en de 'control specification' in het Nederlands is geschreven zijn specifiek toegevoegd.

Toelichting kolom 'Compliance eis'

- Daar waar een control is gemarkeerd met 'volledig' betekent dit dat de leverancier volledig aan deze control moet voldoen en dat er geen verbeterpunten meer mogen zijn.
- Daar waar een control is gemarkeerd met 'deels' betekent dit dat deze punten nog niet volledig hoeven te zijn geimplementeerd. De leverancier moet op termijn aan deze control voldoen en op dit moment al deze control in een bepaalde mate hebben ingericht.

Voor alle controls geldt daarmee dat het niet acceptabel is als er nog helemaal geen maatregelen zijn getroffen om aan deze control te voldoen.

De kolom 'Consensus Assessment Questions' Is overgenomen uit de Cloud Security Agency (CSA) CAIQ en geeft concrete handreikingen om zelf te toetsen in hoeverre aan de norm wordt voldaan.

De kolom 'ISO27001:2013' is overgenomen uit de Cloud Security Agency (CSA) Cloud Control Matrix (CCM) versie 3.0.1 en bevat een mapping naar de volgens CSA van toepassing zijnde paragrafen uit ISO 27001:2013. De kolom 'Interpretation note' is toegevoegd door de schemabeheerder en dient als illustratie / achtergrondbeschrijving van de betreffende control.

Klik op het pictogram hieronder om de Cloud Control Matrix te openen.

CSA_CCM_v3.0.1
Applicability for Kennis

B Template voor bewerkersovereenkomst

Dit is een modelovereenkomst die dient als voorbeeld.

Onderwijsinstellingen en SAAS-leveranciers kunnen met dit model zelf nadere afspraken maken naar aanleiding van iedere specifieke SAAS-dienst. Aan de inhoud van dit model kunnen geen garanties of rechten worden ontleend.

In dit model is niet ingegaan op de concept Europese "Algemene Verordening Gegevensbescherming".

Ondergetekenden:

[**Onderwijsinstelling**], gevestigd en kantoorhoudende @ADRES@, hierbij vertegenwoordigd door @vertegenwoordigingsbevoegde@, @functie@, hierna te noemen: "**Onderwijsinstelling**",

en

[**cloudleverancier**], gevestigd en kantoorhoudende aan de @ADRES@, hierbij rechtsgeldig vertegenwoordigd door @vertegenwoordigingsbevoegde@, @functie@, hierna te noemen: "**Leverancier**",

hierna gezamenlijk te noemen: "Partijen",

overwegende dat:

a) Onderwijsinstelling gebruik wenst te maken van de Software-as-a-Service dienstverlening van Leverancier *[OPTIONEEL:]* en daartoe een Overeenkomst van [datum] (hierna: Overeenkomst) met Leverancier heeft afgesloten;
b) Onderwijsinstelling in het kader van de uitvoering van de Overeenkomst (persoons)gegevens van de leerlingen, diens ouders en/of relaties van Onderwijsinstelling plaatst in de SaaS-oplossing van Leverancier;
c) Partijen afspraken rondom uitwisseling van (persoons)gegegevens in deze Bewerkersovereenkomst willen vastleggen;

verklaren te zijn overeengekomen als volgt:

Artikel 1. DEFINITIES

1.1 Persoonsgegevens: elk gegeven betreffende of herleidbaar tot een geïdentificeerde of identificeerbare natuurlijke persoon;
1.2 Gegevens: alle andere gegevens (data) niet zijnde persoonsgegevens;

1.3 Betrokkene: degene op wie de Persoonsgegevens betrekking hebben. In geval van een kind jonger dan 16 jaar wordt met Betrokkene diens wettelijk vertegenwoordiger(s) bedoeld.
1.4 SaaS-oplossing: de door Leverancier geboden dienst;
1.5 [naam SaaS-oplossing]: [omschrijving dienst van Leverancier].
1.6 Bewerkersovereenkomst: deze overeenkomst tussen Onderwijsinstelling en Leverancier;
1.7 Overeenkomst: Overeenkomst tussen Leverancier en Onderwijsinstellig betrekking hebbend op de door Leverancier aan Onderwijsinstelling geleverde dienst(en).
1.8 Verwerken: elk soort handeling (of deel daarvan) met betrekking tot Persoonsgegevens.
1.9 Europese Economische Ruimte: alle landen van de Europese Unie, Liechtenstein, Noorwegen en IJsland.
1.10 Wbp: wet bescherming persoonsgegevens.

Artikel 2. Voorwerp van deze Bewerkersovereenkomst

2.1 Leverancier levert [naam Saas-oplossing] aan Onderwijsinstelling.
2.2 Onderwijsinstelling is verantwoordelijke ten aanzien van de aan Leverancier verstrekte en te verstrekken (persoons)gegevens. Leverancier handelt als bewerker in opdracht van Onderwijsinstelling en verwerkt de (persoons)gegevens slechts in opdracht van Onderwijsinstelling.
2.3 De door Onderwijsinstelling aan Leverancier geleverde (persoons)gegevens worden geleverd ten behoeve van [naam Saas-oplossing]. Voor zover Partijen reeds een Overeenkomst hebben gesloten ten aanzien van de Saas-dienst, gelden de bepalingen van deze Bewerkersovereenkomst als aanvulling daarop.
2.4 [OPTIONEEL:]De in het kader van deze overeenkomst uitgewisselde (persoons)gegevens zijn beperkt tot [OMSCHRIJVING of OPSOMMING IN APARTE BIJLAGE].
2.5 Leverancier zal de ontvangen (persoons)gegevens uitsluitend verwerken ten behoeve van de levering van [naam Saas-oplossing] aan Onderwijsinstelling en alleen voor zover het verwerken van die gegevens strikt noodzakelijk is ten behoeve van de dienstverlening van Leverancier.
2.6 Alle (intellectuele) eigendomsrechten, auteursrecht en databankenrecht inbegrepen, op de geleverde (persoons)gegevens, blijven te allen tijde berusten bij de Onderwijsinstelling (dan wel de docent of Betrokkene).
2.7 Partijen komen de Wet bescherming persoonsgegevens na. Voor zover de afspraken tussen Partijen niet voorzien in wettelijk vereiste regelingen, komen Partijen overeen te handelen in overeenstemming met de toepasselijke wet- en regelgeving op het gebied van de bescherming van (persoons)gegevens.

Artikel 3. Looptijd Bewerkersovereenkomst

3.1 De looptijd van deze Bewerkersovereenkomst is gelijk aan de looptijd van de tussen partijen gesloten Overeenkomst. In het geval dat de dienstverlening van Leverancier aan Onderwijsinstelling (nog) voortduurt, loopt deze Bewerkersovereenkomst door.
3.2 Na (tussentijdse) beëindiging van deze Bewerkersovereenkomst, blijven de bepalingen van artikelen 2, 3.3 , 4 en 5 onverkort van toepassing.
3.3 Na beëindiging van de Overeenkomst, en/of na beëindiging van de dienstverlening aan Onderwijsinstelling, is Leverancier gehouden om binnen 30 dagen na beëindiging de door Leverancier verstrekte (persoons)gegevens terug te geven (dan wel om Onderwijsinstelling in de gelegenheid te stellen deze gegevens digitaal te verkrijgen). Eventuele resterende (kopieën van) (persoons)gegevens en/of backups dienen daarop door Leverancier te worden vernietigd.

Artikel 4. Beveiligingseisen

4.1 Leverancier zal zorgdragen voor passende technische en organisatorische maatregelen om (persoons)gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De te nemen maatregelen sluiten aan bij de stand van de techniek en de kosten van de tenuitvoerlegging.

4.2 De veiligheidsmaatregelen bieden een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

4.3 De veiligheidsmaatregelen zijn adequaat en voldoen aan de relevante standaarden en kwaliteitseisen.

4.4 [OPTIONEEL:]Leverancier heeft de volgende beveiligingsmaatregelen geïmplementeerd: [opsomming].

4.5 Leverancier is verantwoordelijk voor het regelen van adequaat beveiligde toegang tot de (persoons)gegevens door Onderwijsinstelling.

4.6 Onderwijsinstelling heeft het recht om in overleg met Leverancier de door Leverancier genomen technische en organisatorische (beveiligings)maatregelen - op kosten van Onderwijsinstelling - te (laten) toetsen door een daartoe gecertificeerd en onafhankelijk auditor. Leverancier heeft alsdan het recht om deze audit – al dan niet op eigen initiatief – uit te laten voeren door een door Leverancier in te schakelen onafhankelijk gecertificeerd auditor die een derdenverklaring afgeeft. Onderwijsinstelling wordt – al dan niet op hoofdlijnen - geïnformeerd over de uitkomsten.

4.7 Leverancier stelt Onderwijsinstelling omgaand op de hoogte over ieder veiligheidsincident.

Artikel 5. Geheimhouding en vertrouwelijkheid

5.1 Op Leverancier rust ingevolge artikel 12 van de Wbp een wettelijke geheimhoudingsverplichting. Leverancier is gehouden de ontvangen gegevens als vertrouwelijk te behandelen.

5.2 Leverancier verplicht zijn (oud) werknemers en/of onderaannemers tot geheimhouding met betrekking tot alle (persoons)gegevens waarvan zij met betrekking tot de levering van [naam SaaS-oplossing] kennis nemen.

5.3 Ingeval Leverancier een derde inschakelt bij de dienstverlening, dan dient de Onderwijsinstelling hier uitdrukkelijk mee in te stemmen, voorafgaand aan het sluiten van een overeenkomst met de derde.

5.4 De verstrekte (persoons)gegevens worden door Leverancier niet zonder voorafgaande toestemming van Onderwijsinstelling aan derden ter beschikking gesteld, tenzij Leverancier daartoe krachtens enige wetsbepaling, voorschrift of andere regelgeving verplicht is, of indien de bekendmaking en/of verstrekking in het kader van dienstverlening noodzakelijk is.

5.5 Indien Leverancier een verzoek of een bevel van een Nederlandse of buitenlandse toezichthouder of een opsporings-, strafvorderings- of nationale veiligheidsinstantie ontvangt om (inzage in) (persoons)gegevens te verschaffen, waaronder maar niet beperkt tot een verzoek op grond van de USA Patriot Act, dan zal Leverancier de Onderwijsinstelling onverwijld informeren. Bij de behandeling van het verzoek of bevel zal de Leverancier alle instructies van de Onderwijsinstelling in acht nemen (waaronder de instructie om de behandeling van het verzoek of bevel geheel of gedeeltelijk aan de Instelling over te laten) en alle redelijkerwijs benodigde medewerking verlenen.

5.6 Voor zover Leverancier (persoons)gegevens aan anderen dan Onderwijsinstelling levert, zal Leverancier met deze derde gelijksoortige bepalingen als in deze bewerkersovereenkomst omtrent

de verwerking van (persoons)gegevens overeenkomen, tenzij sprake is van een omstandigheid als genoemd in artikel 5.4.

5.7 Leverancier zal haar volledige medewerking verlenen in geval dat een Betrokkene zijn rechten uitoefent op grond van de Wbp of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens. Indien deze Betrokkene met betrekking tot de uitvoering van zijn rechten onder de Wbp direct contact opneemt met Leverancier, dan verwijst Leverancier Betrokkene in eerste instantie door naar Onderwijsinstelling.

5.8 Leverancier draagt er zorg voor dat de ontvangen (persoons)gegevens worden verwerkt (opgeslagen) binnen de Europese Economische Ruimte. Indien dit niet het geval is, mogen de (persoons)gegevens slechts worden verwerkt in een veilig derde land voor zover de wet dit toestaat (een land dat een passend beschermingsniveau biedt). Leverancier zal Onderwijsinstelling (vooraf) actief informeren indien de gegevens buiten de Europese Economische Ruimte worden verwerkt.

5.9 Bij elke schending van de geheimhoudingsverplichting van Leverancier, is deze aan Onderwijsinstelling een direct opeisbare boete van (maximaal) € 50.000,= per overtreding verschuldigd, onverlet de overige rechten op schadevergoeding.

5.10 Leverancier zal Onderwijsinstelling terstond op de hoogte stellen van iedere kennisneming, verstrekking of andere vorm van verwerken van de gegevens, die plaatsvindt in strijd met dit artikel.

Artikel 6. Aansprakelijkheid

6.1 Leverancier is aansprakelijk voor schade of nadeel, voortvloeiende uit het niet-nakomen van deze Bewerkersovereenkomst, voorschriften bij of krachtens wet- en regelgeving aangaande de bescherming van (persoons)gegevens, voor zover de schade of het nadeel is ontstaan door de werkzaamheid als Leverancier voor Onderwijsinstelling.

6.2 Leverancier is gehouden tot het (onmiddellijk) beperken van schade en/of voorkomen van verder nadeel van Betrokkene en/of Onderwijsinstelling.

6.3 [OPTIONEEL:]De totale aansprakelijkheid van Opdrachtgever is beperkt tot het bedrag dat in het respectievelijke geval door de aansprakelijkheidsverzekeraar van Leverancier wordt vergoed.

Artikel 7. Algemeen

7.1 Bepalingen in de algemene voorwaarden, overeenkomsten of (mondelinge) afspraken tussen Partijen, met betrekking tot de bescherming van de verstrekte (persoons)gegevens, die afwijken van hetgeen in deze Bewerkersovereenkomst is geregeld, zijn niet van toepassing.

7.2 Op deze overeenkomst is Nederlands recht van toepassing. Bij een dispuut over de toepasselijkheid van Nederlands recht, zijn de bepalingen van de Dataprotectierichtlijn 95/46/EG (aanvullend) van toepassing.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Onderwijsinstelling,	Leverancier,
Naam:	Naam:
Functie:	Functie:
Datum:	Datum:

C Template voor zelfverklaring cloudleverancier

MANAGEMENTVERKLARING CERTIFICERING EDUKOPPELING

Verklaring behorend bij het Certificeringsschema Edukoppeling en cloud

Inleiding

Een veilige en uniforme manier van gegevensuitwisseling binnen de administratieve keten in het onderwijsdomein is van groot belang. Hiervoor is de Edukoppeling transactiestandaard ontwikkeld die beschrijft hoe de gestructureerde elektronische informatie-uitwisseling in het onderwijs is ingericht. Edukoppeling is een standaard waarmee onderwijsinstellingen, uitvoeringsorganisaties en andere ketenpartijen eenvoudiger nieuwe gegevensuitwisselingen kunnen opzetten.

Bij gegevensuitwisseling met een onderwijsinstelling die gebruik maakt van een cloudoplossing, is het mogelijk dat de technische identiteit afwijkt van de inhoudelijke identiteit. Technisch worden dan gegevens uitgewisseld met de cloudleverancier, terwijl inhoudelijk de gegevens bedoeld zijn voor of gevraagd worden van één van de scholen die gebruik maakt van die cloudoplossing. Binnen de ROSA[6] is met ketenpartijen gezocht naar een duurzame en standaardoplossing die voldoet aan de benodigde beveiligingsnormen. Dit heeft geresulteerd in een certificeringsproces als onderdeel van Edukoppeling. Als eerste stap in dit certificeringsproces moet de cloudleverancier verklaren dat aan een aantal juridische en technische voorwaarden wordt voldaan. Doel hiervan is om vertrouwen te creëren in de betrouwbaarheid van de geleverde cloudoplossing waarbij voldaan wordt aan de minimale eisen waaraan een cloud-toepassing moet voldoen om te mogen worden ingezet als cloudoplossing.

In deze managementverklaring legt de vertegenwoordigingsbevoegde bestuurder en/of manager vast dat naar zijn of haar oordeel de cloudoplossing van aanvrager voldoet aan het Certificeringsschema. Dit oordeel van aanvrager is tot stand gekomen na toetsing van de cloudoplossing aan de normen en uitgangspunten zoals beschreven in het Certificeringsschema.

Verklaring

Aanvrager _____ (naam leverancier), hierbij rechtsgeldig vertegenwoordigd door _____ (naam vertegenwoordiger), _____ (functie), verklaart dat de cloudoplossing van aanvrager, genaamd _____ (naam cloudoplossing), voldoet aan de normen en uitgangspunten zoals genoemd in het Certificeringsschema.

_____

[6] http://www.wikixl.nl/wiki/rosa

Aanvrager heeft de Bijlage D van het Certificeringsschema ingevuld waarop tevens is aangegeven of en in welke mate aan de beschreven normen wordt voldaan, of op welke termijn de aanvrager daar aan zal voldoen. Aanvrager voldoet aan alle onderdelen van het Certificeringsschema waar in de kolom “Compliance eis” is gemeld dat daar “volledig” aan moet worden voldaan. Het Certificeringsschema is als bijlage bij deze verklaring gevoegd en maakt daar onlosmakelijk onderdeel van uit.

Aanvrager verklaart voorts dat:

1. de services waarmee gegevens conform Edukoppeling met andere ketenpartijen worden uitgewisseld, voldoen aan de Edukoppeling transactie-standaard (interoperabiliteit);
2. voldoende maatregelen zijn genomen om onrechtmatige en/of onbevoegde toegang door derden en/of eigen (oud-)medewerkers tot de in de cloudoplossing aanwezige gegevens te voorkomen;
3. maatregelen zijn genomen om vermenging van gegevens van verschillende gebruikers van de cloudoplossing te voorkomen;
4. een log of audittrail wordt vastgelegd per klantomgeving ten behoeve van het eventueel uitvoeren van digitaal (forensisch) onderzoek en audits;
5. de (toegang tot de) cloudoplossing, alsmede opslag van gegevens in die cloudoplossing, voldoet aan de eisen van de Wet bescherming persoonsgegevens[7] en de Dataprotectierichtlijn (95/46/EC[8]);
6. tussen aanvrager en de onderwijsinstellingen die gebruik maken van de cloudoplossing, een bewerkersovereenkomst is gesloten (zie voor een model, Bijlage B bij het Certificeringsschema);
7. een nieuwe Managementverklaring (met bijlage) zal worden ingediend in geval van ingrijpende wijzigingen of updates aan de cloudoplossing, indien die aanpassingen van invloed (kunnen) zijn op de normen en uitgangspunten zoals opgenomen in het Certificeringsschema.

Aanvrager gaat er mee akkoord dat de Beheerder Register – bij wijze van steekproef - kan besluiten om de cloudoplossing van aanvrager te laten toetsen door een onafhankelijk en gecertificeerd ICT-auditor. Indien uit deze audit blijkt dat de cloudoplossing niet voldoet aan de normen en uitgangspunten van het Certificeringsschema, kan deze verklaring worden geweigerd en vervalt de certificering van aanvrager. Bij gebreke van een geldige certificering, worden er dan via aanvrager geen gegevens meer uitgewisseld.

Aldus opgemaakt en getekend op _____ (datum) te _____ (plaats),

_____ (handtekening)

_____

[7] http://wetten.overheid.nl/BWBR0011468/

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML

(naam voluit)
(functie)

Bijlage: ingevuld Certificeringsschema

Deze ingevulde en getekende verklaring (met bijlage) dient

- per post te worden toegezonden aan Paletsingel 32, 2718 NT Zoetermeer, én
- per e-mail aan info@sionderwijs.nl

D Template voor bijlage bij zelfverklaring

Klik op het pictogram hieronder om de template te openen.

Bijlage D van
Edukoppeling Certifice

E Veelgestelde vragen

Vraag: Is de Cloud Control Matrix (CCM) van Cloud Security Alliance wel een passend kader?
Antwoord: De CCM is een specifieke normenkader voor cloud dienstverlening.

Het vakgebied is zeker nog niet volwassen en er is nog geen algemeen geaccepteerde marktstandaard. Wereldwijd wordt het CCM normenkader het meest gebruikt en het actiefst beheerd / doorontwikkeld. De toonaangevende cloudbedrijven hebben dit normenkader omarmd.

Vraag: Aan welke eisen moet nu minimaal wel of niet worden voldaan? / Wat is nu de echte basisset van alle normen? / Hoe moet ik norm XYZ interpreteren?
Diverse vragen zijn ontvangen over prioriteiten en formuleringen. Deze vragen zijn begrijpelijk en passen bij het initiële stadium waarin het schema zit en de pioniersrol die wordt vervuld.

Op dit moment is de ervaring met het toepassen van de norm nog beperkt, bij alle partijen (leveranciers, afnemers en andere stakeholders). De praktijk zal moeten uitwijzen welke normen helder en duidelijk zijn en aan welke normen leveranciers kunnen voldoen.

Bij een eerste evaluatieronde moet worden besproken welke generieke CCM formuleringen en specifieke 'interpretation notes' aan de normen worden toegevoegd. Ook moet bijvoorbeeld worden vastgesteld:

- welke normen als basisset moeten dienen,
- welke normen toegevoegde waarde hebben,
- welke normen moeten worden aangescherpt en
- waar aanvullende normering op zijn plaats zou zijn.

Vraag: Wat is de overlap met ISO 27001 en ISAE 3402?
Korte antwoord: de overlap is beperkt, een self-assessment tegen het CCM normenkader kan naadloos worden geïntegreerd in een ISO 27001: 2013 certificering of ISAE 3402.

Uitgebreide inhoudelijke toelichting:
De ISO 27001 standaard is een wereldwijd leidende standaard op het gebied van informatiebeveiliging. De standaard stelt eisen aan een management systeem voor informatiebeveiliging (een 'ISMS'). Daarbij worden in een Annex A specifieke controls genoemd. ISO 27001: 2013 kent een significante wijziging: "The two primary sources for the Statement of Applicability are the risk assessment and Annex A of the standard (in reality the Table of Contents of the ISO 27002 standard). ***Other sources are the controls that currently exist in the organization and external security requirement that the organization has to comply with***."

Dit is een belangrijke doorbraak: in eerdere versies van 27001 waren de controls uit Annex A niet specifiek genoeg om te passen bij de dienstverlening van de te certificeren organisatie. In de

nieuwe versie kunnen ook specifieke controls worden toegevoegd, voor zover zij als relevante controls worden benoemd in de risico-analyse. Dit betekent dat voor cloud dienstverleners relevante cloud gebaseerde normenkaders onder de ISO 27001 kunnen worden opgenomen en (bij certificering) door een onafhankelijke auditor worden getoetst. Hiermee kunnen leveranciers de CCM control matrix adopteren en later in een ISO 27001 certificeringstraject laten toetsen. Een onafhankelijk ISO27001 certificaat waarbij tevens de CCM controls zijn getoetst kan daarmee de zelfverklaring vervangen.

Wat is ISAE 3402: ISAE3402 is een internationale assurance standaard uitgegeven door de International Federation of Accountants (IFAC). In een ISAE3402 rapport is opgenomen hoe de accountant heeft getest en zijn uiteindelijke accountantsverklaring bij het ISAE3402-rapport.

In ISAE3402 type I rapport wordt uitsluitend gerapporteerd over het bestaan van het control framework (de beheersmaatregelen) op een moment. In een ISAE3402 type II rapport wordt over zowel het bestaan als de werking gerapporteerd over een periode van minimaal zes maanden.

ISAE bevat geen specifiek normenkader. Het CCM normenkader kan als normenkader aan de (onafhankelijke) ISAE 3402 worden toegevoegd. Een ISAE3402 verklaring (type I of II) kan daarmee als vervanger van de zelfverklaring dienen.

Informatiebeveiliging is een integraal onderdeel van ISAE3402. Deze informatiebeveiliging moet zodanig ingericht zijn dat deze 'veilig' is voor de gebruikersorganisatie. ISO27001 wordt feitelijk volledig 'gedekt' door ISAE3402. Aan de andere kant heeft ISAE3402 alleen betrekking op de processen die een organisatie uitbesteedt en niet op de 'eigen' bedrijfsprocessen, deze vallen buiten de scope. De vraag is dan wel in hoeverre afnemers belang hechten aan de eigen processen van een organisatie, want ook ISO27001 wordt voornamelijk gebruikt voor profilering richting 'derden'. Het belangrijkste verschil is eigenlijk dat ISO27001 beperkt bruikbaar is voor externe accountants. Een belangrijk pluspunt van ISO27001 is dat er wel gedetailleerde voorschriften zijn die bij ISAE3402 ontbreken. De kwaliteit van een ISAE3402 rapport is daardoor afhankelijk van degene die hem opstelt en de uiteindelijke controleur.

Vraag: Wat is het verschil tussen het schema en het SURF normenkader voor cloudservices in het hoger onderwijs?

Het vertrekpunt van het SURF kader is de Wet Bescherming Persoonsgegevens, het vertrekpunt van het Certificeringsschema Edukoppeling is de aard van de (cloud) dienstverlening
Effect is dat in het SURF kader meer in kwalitatieve termen wordt gesproken (‘adequaat, onverwijld, in eerste instantie’) en in het Edukoppeling kader over meer technisch inhoudelijke termen.
Je zou kunnen zeggen dat het schema een verdere uitwerking is van het normenkader ten aanzien van de eisen die gesteld worden aan de leveranciers. Het SURF normenkader stelt ook eisen aan onderwijsinstellingen, dit is in het schema niet het geval.