
Voor:	Standaardisatieraad, Edustandaard
Van:	Marcia van Oploo (Bureau Edustandaard)
Datum	27-6-2017
Betreft	Inbeheername van Certificeringsschema informatiebeveiliging en privacy ROSA v.2017

1. Samenvatting

De afspraak Certificeringsschema informatiebeveiliging en privacy ROSA v.2017 (afgekort CS v.2017) wordt ter inbeheername ingediend bij edustandaard. De nieuwe versie komt in de plaats van de, in 2015 door de standaardisatieraad vastgestelde, 1.1 versie van het schema. Waar de 1.1 versie alleen in relatie met edukoppeling gebruikt werd, kent CS v.2017 een veel ruimer toepassingsgebied. De algemene beschrijving van het certificeringsschema licht dat als volgt toe:

“Binnen het onderwijs vervult ict een belangrijke rol. Op verschillende manieren wordt gebruik gemaakt van ict-toepassingen voor onderwijskundige of onderwijsondersteunende producten en diensten. De aard en inhoud van deze ict-toepassingen kunnen onderling sterk verschillen, maar zij hebben als gemeenschappelijk kenmerk dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevensbewerking cruciaal is. Ook de toegenomen aandacht en strengere wetgeving rondom privacy dwingt alle partijen in de onderwijsketen expliciet aandacht te besteden aan informatiebeveiliging en privacy (IBP). Onderwijsinstellingen moeten erop kunnen vertrouwen dat (publieke of private) organisaties die ict-toepassingen leveren in het onderwijs persoonsgegevens op een veilige manier bewerken.

Voor onderwijsinstellingen is het echter niet eenvoudig om vast te stellen of een leverancier de juiste maatregelen heeft genomen. Omgekeerd is het voor leveranciers niet eenvoudig om aan te tonen dat zij tenminste aan de minimale eisen voldoen. Het hanteren van een eenduidige meetlat moet dit probleem oplossen. Bestaande ‘normenkaders’ bieden hierbij niet de helderheid en transparantie die nodig is om met partijen in een keten afspraken te maken.

Daarom hebben ketenpartijen in het onderwijsdomein gezamenlijk het ‘certificeringsschema informatiebeveiliging en privacy ROSA’ opgesteld. Deze standaard is onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA1) en wordt binnen Edustandaard beheerd door de werkgroep IBP. Deze werkgroep bestaat uit IBP-specialisten uit de onderwijsketen en vertegenwoordigt zowel onderwijs als leveranciers. Via deze werkgroep kunnen alle partijen in de onderwijsketen invloed uitoefenen op de inhoud van de standaard.”

2. Proces

De 1.1 versie van het CS is in samenhang met edukoppeling ontstaan vanuit het programma SION. Aan het eind van het SION programma werd al de beweging ingezet om het toepassingsgebied te vergroten. Naast de inhoudelijke verandering werd ook een verandering in samenwerking gezocht en gevonden. Het CS v.2017 is het product van een publiek/private samenwerking, in de edustandaard werkgroep IBP zijn zowel publiek als private partijen vertegenwoordigd. Afgelopen jaar is bij een aantal partijen pilots uitgevoerd. Input uit deze pilots heeft het schema beter gemaakt. Verdere uitrol en daarmee feedback op het schema blijft enigszins hangen omdat partijen wachten op een formeel vastgestelde versie.

3. Gebruik en implementatie

In de voorbereiding zijn bij meerdere pilots zijn uitgevoerd en is het schema door meerdere partijen beproefd. Feedback hieruit is meegenomen in de laatste versie van het schema. Voor uitrol van CS v.2017 is een implementatieplan opgesteld. Dit plan is besproken en vastgesteld in de vergadering van Edu-k van 21-6-2017. De hele documentatieset voorziet in alle nodige aspecten van de implementatie, in de procesbeschrijving staat beschreven welke stappen nodig zijn en wat de bijbehorende inspanning is.

4. Advies Bureau Edustandaard

Bureau Edustandaard beoordeelt de afspraak Certificeringsschema informatiebeveiliging en privacy ROSA v.2017 als **Voldoende, met aandachtspunten**.

Het Certificeringsschema v.2017 informatiebeveiliging en privacy ROSA v.2017 (CS v.2017) is een afspraak die een gedetailleerde uitwerking kent. De begeleidende documenten schetsen de context en het beheerproces van de afspraak, waarbij de focus op structurele feedback op de afspraak positief opvalt. De classificatietool is bedoeld als een praktisch hulpmiddel waarmee leveranciers hun audit kunnen (laten) uitvoeren, en onderwijsinstellingen desgewenst transparantie biedt. De vorm (Excel-formulier) kan professioneler, maar voldoet voor de fase waarin het Certificeringsschema v.2017 zich bevindt. Het toetsingskader is met zorg tot stand gekomen en met consultatie van een brede groep stakeholders. Al met al beoordelen wij de afspraak als voldoende, met aandachtspunten.

Om adequaat in te kunnen springen op nieuwe dreigingen is gekozen om de doorontwikkeling van het Certificeringsschema v.2017 kortcyclisch te laten plaatsvinden. Tussentijdse versies bieden advies over de laatste informatiebeveiliging en privacy-inzichten, de eenmaal per jaar formeel vastgestelde versie door Edustandaard geldt als baseline waar partijen aan gehouden kunnen worden³. Deze werkwijze wijkt af van de standaard processen van Edustandaard, maar is gezien het afwijkende karakter van het Certificeringsschema v.2017 te verdedigen. Het aandachtspunt hierbij is wel om in praktijk te ervaren hoe het kortcyclisch werken voldoet voor alle partijen. Is voor leveranciers helder waar zij aan moeten voldoen, en voor onderwijsinstellingen waarop zij kunnen toetsen? En wat is de status van de tussentijdse versies in de praktijk, worden ze überhaupt opgepakt of worden ze misschien zelfs leidend? De antwoorden hierop kunnen aanleiding geven om het standaardisatieproces anders in te steken. Om deze reden stellen wij voor in de roadmap van het Certificeringsschema v.2017 een evaluatie op te nemen om de kortcyclisch werkwijze na het eerste jaar te toetsen en de werkwijze indien nodig aan de bevindingen aan te passen.

5. Advies werkgroep

Alle leden van de werkgroep IBP staan achter de ingediende CS v.2017 en geven een positief advies over inbeheername van de afspraak.

6. Advies Architectuurraad

De Architectuurraad geeft een positief advies over de registratie van de afspraak. Bureau Edustandaard heeft een zogenaamde ROSA-architectuurscan uitgevoerd op CS v.2017, ten behoeve van bespreking door de Architectuurraad. Hierin zijn de belangrijkste architectuuraspecten in kaart gebracht met als referentie de ROSA. Dit heeft (strategische) adviezen opgeleverd aan de indiener, andere ketenpartijen, en verbeteringen aan de ROSA.

7. Gevraagd besluit

De leden van de Standaardisatieraad wordt gevraagd om in te stemmen met de inbeheername van de afspraak CS v.2017