



Compliance diensten

vanuit het programma Cyberveiligheid mbo

Martijn Bijleveld (MBO Digitaal)
Niels Dutij (MBO Digitaal)
Sandy Janssen (SURF)

27 januari 2023

Veiligheidswaarborgen van onze (cloud)leveranciers
centraal geregeld met verwerkersovereenkomsten,
DPIA's, pentests en audits



Programma Cyberveiligheid mbo

- Gecoördineerd door MBO Raad / MBO Digitaal
- Afstemming met:
 - netwerk IBP (via regiegroep IBP)
 - contactpersonen SURF (via CSC-overleg)
 - Innovatiezone SURF (via regiegroep IZ)
- Uitvoering in principe door- of samen met SURF
 - samenwerkingsovereenkomst
- Samenwerken met FO en HO waar zinvol
- Subsidieaanvraag 24 mln goedgekeurd
- Per 1 oktober 2022 gestart



Programma Cyberveiligheid mbo

1. Identificeren van dreigingen en risico's (*identify*)
2. Beschermen tegen cyberrisico's (*protect*)
3. Detecteren van onregelmatigheden (*detect*)
4. Reageren op incidenten (*respond*)
5. Herstellen van incidenten (*recover*)
6. Leveranciersmanagement



Programma Cyberveiligheid mbo

1. Identificeren van dreigingen en risico's (*identify*)
2. Beschermen tegen cyberrisico's (*protect*)
3. Detecteren van onregelmatigheden (*detect*)
4. Reageren op incidenten (*respond*)
5. Herstellen van incidenten (*recover*)

6. Leveranciersmanagement

- Centraal beoordelen overeenkomsten
- Centraal uitvoeren DPIA's, pentests en audits
- Ontwikkelen mbo-brede applicatiecatalogus



Leveranciersmanagement IBP

- Gestart in 2017 met verwerkersovereenkomsten (werkgroep)
 - Onderhoud blijkt lastig
 - Behoeftte aan meer: ook DPIA's, audits en pentests
- Centraal budget?

Subsidie vanuit programma Cyberveiligheid 2022-2027

- 700.000/jr voor compliance diensten SURF
- 300.000/jr voor mbo-specifieke trajecten

Wat pakken we nu al op?

- Inventarisatie van kernleveranciers MBO
- 1. Zijn alle artikelen uit de verwerkersovereenkomst van het Privacy Convenant ongewijzigd overgenomen? Zo nee, is dan aangegeven waarom artikelen niet zijn overgenomen?
- 2. Is de privacy bijsluiter ingevuld op basis van het format uit het convenant? Waarom is er afgeweken?
- 3. Zijn er beveiligingscertificaten, DPIA's, pentesten of andere rapportages op basis waarvan waarborgen op het gebied van IB en P worden geleverd? Wordt het ROSA-certificeringsschema gebruikt of zijn er andere relevante beveiligingsscertificaten?
- 4. Is er een (standaard) SLA van toepassing? Wat zijn de belangrijkste bevindingen?
- 5. Zijn er voor mbo-instellingen specifieke aandachtspunten bij het gebruik van deze dienst/dit systeem?

Inventarisatie kernleveranciers

- Eduarte - Topicus
 - Osiris - CaCl
 - Talentscan - AMN
 - Startmeter - NOA
 - MTO – Effectory
 - See – Pearson
 - Onstage – Xebic
 - Xedule – Advitrae
-
- Input gevraagd van het netwerk IBP voor op te pakken nieuwe applicaties

Landelijke DPIA's / IT-audits / Pentesten MBO

- Via SURF Compliancy diensten
- Specifieke MBO-systemen komt een apart programma nog in samenwerking met SURF;
- Eerste gegunde opdracht aan ICTRecht voor opstellen landelijke DPIA voor Eduarte.
- Input gevraagd van het netwerk IBP voor op te pakken nieuwe applicaties

SURF Leveranciers Compliance Dienstverlening

Sandy Janssen SURF

Sandy.janssen@surf.nl

SURF

Kader voor Leveranciers Compliancy Dienstverlening

SURF Procurement & Contracting ontwikkelt de Leveranciers Compliancy Dienstverlening voor applicaties die voor het merendeel van de leden relevant zijn, en verzorgt compliance checks en afspraken.

- **Evolutie:** De werkzaamheden op het gebied van privacy en security compliancy zijn in een paar jaar sterk geëvolueerd, onder meer door wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG) en het ongeldig verklaren van Privacy Shield.
- **Wettelijke verantwoordelijkheid:** Instellingen zijn verantwoordelijk voor hun data en moeten hiermee omgaan conform wet- en regelgeving. Bij inbreuk op persoonsgegevens zijn er risico's op boetes, reputatieschade en aansprakelijkheidsstellingen. Instellingen maken zich hierover zorgen en kunnen dit onvoldoende zelf invullen.
- **Toetsen leveranciers:** Het is nodig om bij leveranciers te toetsen hoe zij data van de instellingen verwerken en hierover met hen afspraken te maken.
- **Huidige situatie:** Instellingen voeren het merendeel van dit compliance werk nu **individueel** uit: hetzelfde werk, voor dezelfde applicaties, waarvoor de benodigde expertise schaars en kostbaar is.
- **Oplossing – een nieuwe dienst:** Het gezamenlijk oppakken levert kostenbesparing op, daarnaast hebben we een grotere onderhandelingspositie hebben t.a.v. de leveranciers.

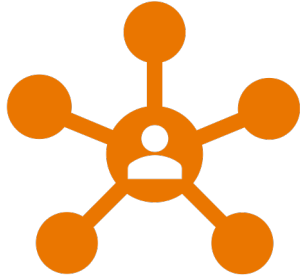
Leveranciers Compliancy Dienstverlening

- **Ambitie:** De ambitie voor de compliance dienstverlening is opgenomen in de SURF strategie, Jaarplannen 2022 & Innovatiezone State of the Art Cyberveiligheid, het programma Cyberveiligheid MBO 2022-2027 van MBO digitaal en past bij de aandacht vanuit de Overheid, AP en maatschappij voor privacy en security binnen de onderwijssector.
- **Interne afstemming:** SURF bespreekt deze plannen met de relevante gremia: CSC Inkoop, Privacy en Security Linking Pins, in de Innovatiezone State of the art (cyber)veiligheid, Taskforce Beyond Privacy Shield. Business voorstel ligt voor bij SPA en RvB, en daar waar nodig met de ledenraad; om op basis van coöperatief vastgestelde prioriteiten, keuzes te maken, kosten te verdelen en zo de expertise en vraag te bundelen.
- **Externe samenwerking en afstemming:** Koepels (VH, UNL, MBOraad), OCW, AP over de rol van SURF. Steunen collectieve aanpak. Sluit aan bij de ambitie van MBO Digitaal
- Samenwerkingsverbanden met: SLM Rijk, SIVON/Kennisnet, SLB, SURF Taskforce Beyond Privacy Shield, SCIRT / SCIPR network, UPI / inkoop netwerk, intern SURF, NRENs, GEANT & MBO Digitaal

Wapenfeiten:

Er zijn al goede resultaten geboekt met dit compliance werk richting leveranciers die een nationale impact hebben: o.a. Google, Microsoft en Zoom.

Samenwerkingen / kruisverbanden



- **Intern**
 - Dienstverlening inkoop Procurement & Contracting
 - Innovatiezone State of the Art (Cyber)veiligheid
 - Team K&IJ



- **Netwerken:**
 - SURF Taskforce Beyond Privacy Shield
 - SCIRT / SCIPR netwerk
 - UPI / inkoop netwerk

- **Samenwerkingspartners**
 - SIVON/Kennisnet
 - SLM Rijk
 - GÉANT
 - NRENs
 - Koepels
 - AP
 - OCW
- **Voor MBO: Samenwerking met MBO Digitaal**

Wat gaan we doen

SURF Procurement & Contracting ontwikkelt de Leveranciers Compliancy Dienstverlening voor applicaties die voor het merendeel van de leden relevant zijn, en verzorgt compliance checks en afspraken.



Kaders en Risico analyses

(o.a. via DPIA's en DTIA's, security checks), waaronder voor data transfers buiten de EER, met juridisch en technisch onderzoek, en gestandaardiseerde toetsingskaders waarop leveranciers getoetst worden.



Afspraken met leveranciers

Afspraken met de leverancier, waarin (privacy)risico's worden gemitigeerd en toezicht op naleving, door bijv. Afsluiten van verwerkersovereenkomst en afspraken over security maatregelen.



Informatie, ondersteuning en toezicht

voor implementatie en gebruik bij de instellingen & toezichthouden op de naleving door de leverancier en herziening van gemaakte afspraken.

SURF Procurement & Contracting biedt zo de bouwstenen, waarmee een instelling zelf een goede afweging kan maken en tot een veilig gebruik van (cloud)software kan komen.

Compliance trajecten



Voor circa 2.1 miljoen per jaar

3 kleine trajecten [300.000 euro]

3 middelgrote trajecten [600.000 euro]

2 grote trajecten [700.000 euro]

+ kosten voor onderhoud van trajecten / toezicht [500.000 euro]

COMPLIANCE TRAJECT (Privacy en Security)	KOSTEN	
Klein	€ 100.000	Klein: Juridische analyse, verwerkersovereenkomst, Scope: SURFleden, doorlooptijd gemiddeld 5 maanden, toezicht op leverancier zal beperkt zijn.
Middel (o.a. Zoom)	€ 200.000	Middel: Juridische analyse, technisch onderzoek, verwerkersovereenkomst, Scope: SURFleden/onderwijssector, doorlooptijd gemiddeld 10 maanden, toezicht op de leverancier is uitgebreid
Groot nationaal belang (o.a. Google)	SURF deel € 350.000 Samen met het Rijk en SIVON totaal 1.000.000	Groot: Juridische analyse, technisch onderzoek, verwerkersovereenkomst, Scope: SURFleden/onderwijssector/BV Nederland, doorlooptijd gemiddeld 15 maanden, toezicht op de leverancier is uitgebreid
Toezicht/audits op de naleving door leveranciers	500.000	

Financiering voor structurele dienstverlening



Goedgekeurd: een
financiële bijdrage vanuit
de leden



Benodigd: circa
2.1 miljoen per
jaar



voor gezamenlijk
leveranciers compliance
werk via SURF

Dat deden we tot nu toe ad hoc; met succes zoals met ZOOM. We vragen nu om een structurele bijdrage van de leden:

- Iedere lid betaalt een jaarlijkse bijdrage die wordt opgenomen in de basisvergoeding van SURF
- Kosten worden berekend aan de hand van deze basisvergoeding:

Financieringsmodel: op basis van aantal FTE en aantal studenten. (sluit aan bij basisvergoeding inkoop)

- Berekening op basis van FTE medewerkers + aantal voltijd studenten + deeltijdstudenten (factor 0.5) = <aantal>
- <aantal> x 1,50 (1,50 euro per FTE/student) = <bijdrage>
- Op basis van de registratie van de aantallen met een minimum en maximum [evt. per sector]
De bijdrages is maximaal 45.000 euro per MBO instelling.

- Bijdrage vanuit de MBO instellingen bedraagt rond de 700.000 euro
- 2022—2027 gefinancierd via subsidie vanuit programma Cyberveiligheid MBO 2022-2027

Voordelen

Deze bijdrage is voor een individuele instelling een lager bedrag dan 1 DPIA traject uitvoeren op één leverancier waarbij alle technische en juridische aspecten worden doorgelicht en alsmede het toezicht op de naleving van de afspraken wordt ingericht. – *ter illustratie: een traject*

zoals ZOOM kost gemiddeld 200.000 euro.

Onderhoud en toezicht op compliance trajecten

- Het werk is niet klaar nadat de DPIA/risicoanalyse is uitgevoerd. Voor elk dossier dat we oppakken zal in de jaren daarna onderhoud en toezicht noodzakelijk zijn. Dit maakt dat de kosten hiervoor blijvend zijn en door de jaren heen zullen toenemen.
- **Voorbeeld:**

Compliance trajecten Kosten ontwikkeling	IMPACT	Jaar 1	Jaar 2	Jaar 3	Jaar 4	Jaar 5
Pakket 6	Midden			R	C	H
Pakket 5	Groot			R	C	H
Pakket 4	Midden		R	C	H	C
Pakket 3	Groot		R	C	H	C
Pakket 2	Midden	R	C	H	C	H
Pakket 1	Groot	R	C	H	C	H

R = risico analyses

C = controle afspraken

H = herevaluatie contracten en audit

Wordt gewerkt aan: uitvoering, organisatie – hoe bepalen we welke dossiers er opgepakt worden?



- Compliance Dienstverlening inventariseert bij de gremia en de Leden **bepalen** gezamenlijk de wensen voor compliance dossiersinhoudelijke behoeftes vanuit;



- SURF (Compliance dienst) **bundelt** deze wensen in een overzichtslijst en komt met een beargumenteerd voorstel voor de uitvoering en legt deze voor aan een *adviesgroep (bijv. CSC voorzitters en/of regiegroep State of the Art Cyberveiligheid)* om de binnengekomen aanvragen te **prioriteren** op onder meer;



- De Leden **besluiten** gezamenlijk over welke trajecten worden uitgevoerd

Door de CSC gremia, via de door hen gemandateerde Linking Pins (inkoop, privacy, security)

- Innovatiezone State of the art (cyber)veiligheid
- SURF Taskforce Beyond Privacy Shield
- SCIPR
- CSC Inkoop Linking Pins
- MBO-Digitaal

- Mogelijkheid samengewerken met Rijk /SIVON
- Gebruik en vraag/urgentie binnen sectoren
- Gesignaleerde issues zoals locatie dataopslag of incidenten bij leverancier.

Wensen voor vervolg trajecten genoemd door de leden

		Stakeholders		
Wensen voor compliance trajecten	IMPACT	SURFleden	Onderwijsbreed	BV Nederland
Eduarte	Midden	x		
Qualtrics	Midden	x		
Miro	Klein	x		
Blackboard	Midden	x	x	
Urkund	Midden	x		
OSIRIS	Midden	x	x	
Kaltura	Midden	x	x	
Zoom	Midden	x	x	x
AWS	Groot	x	x	x
Citrix	Midden	x	x	x
Adobe	Groot	x	x	x
VMware	Groot	x	x	x
AFAS	Groot	x	x	x

Inventarisatie kernleveranciers

- Eduarte - Topicus
 - Osiris - CaCl
 - Talentscan - AMN
 - Startmeter - NOA
 - MTO – Effectory
 - See – Pearson
 - Onstage – Xebic
 - Xedule – Advitrae
-
- Input gevraagd van het netwerk IBP voor op te pakken nieuwe applicaties

Planning

- 13 dec 2022
- Plan versie 0.7
Goedgekeurd
door SURF RvB

- 14 mrt 2023
Plan versie 1.0
naar SURF
portfolio
adviescommissie

- 5 april 2023
Goedkeuren
Business Model
1.0 Door RvB



- Goedgekeurd:
opnemen in portfolio
SURF
- Opbouwen
dienstverlening



- Q1: Opbouwen
dienstverlening
- Inrichten Governance
- Uitvragen wensen
voor compliance
trajecten
- Start werving
expertise

Vragen & discussie

