

# Dypdykk i cybersikkerhet: støtte skolenes personvern og eierskap til egne opplysninger

SAMMENDRAG

30 June 2025

## Problem og kontekst

Personvern og cybersikkerhet har blitt viktige temaer etter hvert som bruken av digitale læringsverktøy og EdTech-tjenester øker i nederlandske skoler. Skolene mangler imidlertid ofte kunnskap, tid eller standardiserte prosesser for å håndtere disse risikofaktorene på en effektiv måte. Et desentralisert skolesystem, der skoleeierne opptre uavhengig, kompliserer saken ytterligere ved at det er store variasjoner i den digitale sikkerheten fra institusjon til institusjon.

For å bøte på dette iverksatte SIVON, støttet av Kennisnet og det nederlandske utdanningsdepartementet, en serie nasjonale tiltak for å styrke datastyringen og cybersikkerheten på barne- og ungdomstrinnet. Ett av disse initiativene, Deep Dive-prosjektet, ble lansert for å evaluere de eksisterende digitale sikkerhetsrutinene og hjelpe skolene med å utforme tilpassede forbedringsplaner.

## Deep Dive-prosjektet

Deep Dive-prosjektet ble gjennomført av SIVON og vurderte informasjonssikkerheten hos 15 skoleeiere (som representerte 290 skoler og 80 000 elever). De benyttet et nyutviklet [standardrammeverk](#) som besto av 69 faktorer på 15 domener (f.eks. risikostyring, sikkerhetsretningslinjer, håndtering av hendelser). Blant de viktige punktene var:

1. **Vurdering av minimumsverdier.** Sertifiserte revisorer brukte to dager på å evaluere hver skoleeiers personverninfrastruktur og graderte dem på en skala fra 1 til 4. Skolene fikk karakterer mellom 1,3 og 2,5, noe som avslørte store forskjeller.
2. **Spesialtilpassede forbedringsplaner.** Funnene ble drøftet med relevante aktører (skoleledelse, IKT-personale, HR), og det ble gitt skreddersydde anbefalinger. Skolene mottok risikosammendrag og vedtok spesifikke tiltak basert på behov og modenhetsnivå.
3. **Opplæring og kapasitetsoppbygging.** Skolene ble oppmuntret til å gi de ansatte opplæring, definere rollene innenfor digital sikkerhet, visualisere IKT-miljøene og utvikle retningslinjer for e-post og fillagringsprotokoller.
4. **Eksempel – De Rank.** Denne barneskolen utarbeidet i samarbeid med SIVON en handlingsplan for datasikkerhet for å styrke IKT-opplæringen og forbedre kartleggingen av den digitale infrastrukturen og ansvarsfordelingen.

Etter Deep Dive tilbød SIVON og Kennisnet en **omfattende pakke av tjenester** for å styrke den digitale sikkerheten på hele skolen.

- **Felles innkjøp** av EdTech-verktøy, -tjenester og infrastruktur til lavere pris. Dette gjorde det for eksempel mulig å forhandle om prisen, noe som i ett tilfelle førte til 40 % lavere pris på interaktive whiteboards.
- **Utarbeide personvernavtaler** for å gjøre det enklere å følge regelverket.

- **Beredskapsenheter** som kan bistå ved hendelser med skadevare eller løsepengevirus.
- **Fagnettverk** som «Network IBP» (900 medlemmer) der man kan utveksle praksis.
- **Tjenester innen risikoanalyse** og praktiske retningslinjer for innføring av retningslinjer for cybersikkerhet.

Parallelt med dette ga **nasjonale forhandlinger med teknologigigantene (som Google, Microsoft, Apple)** viktige resultater som garantier om eierskap til opplysninger og begrensning av kommersiell bruk av data. Disse forhandlingene ble basert på [vurderinger av personvernkonsekvenser \(DPIA\)](#) ledet av SIVON.

## Hva vi har lært

- Deler av organiseringen, risikostyringen og systemutviklingen var jevnt over svake. Et vanlig problem er at skolene ikke har noen kriseplan og gode backup-rutiner. De har heller ikke rutiner for oppgaver knyttet til datasikkerhet. Skolenes vanligste behov ved første øyekast er å øke kunnskapene om datasikkerhet, sentralisere administrasjonen av programvare-som-en-tjeneste-leverandører og utarbeide flere retningslinjer.
- Skolene er mer modne når det gjelder håndtering av hendelser, fordi mange skoleeiere outsourcer datasikkerhetsarbeidet til profesjonelle leverandører.
- De fleste skoler oppfylte ikke minimumsstandardene. Særlig mindre skoler hadde problemer på grunn av begrenset kapasitet.
- Skolene prioriterer ofte verktøyenes funksjonalitet fremfor å ivareta personvernet, for eksempel hvordan personopplysningene blir lagret eller behandlet.
- Skolene etterlyste tydeligere språk og mer relevante referansepunkter fra SIVON, særlig for dem som ikke utvikler egen programvare. Også sentralisert risikostyring for leverandører ble foreslått som mer gjennomførbart enn å gjøre arbeidet på skoleeiernivå.
- Tillitsbaserte, offline nettverksarrangementer kan bidra til åpenhet for mindre modne skoler og bidra til produktiv utveksling av beste praksis.
- Det første utvalget hadde en overvekt av skoler som allerede var interessert i, eller som jobbet med digital sikkerhet. Uansett, siden piloten omfattet 290 skoler, ble den et omfattende og informativt prosjekt for SIVON.

Ved å kombinere regulatoriske rammeverk, praktiske verktøy, sentraliserte forhandlinger og støtte på skolenivå viser denne nederlandske modellen hvordan opplæringssystemene kan iverksette hensiktsmessige tiltak for å beskytte personopplysninger i skolen og inngå innkjøpsavtaler som er mer fordelaktige for skolene.

Selv om de første evalueringene viste betydelig rom for forbedring, banet den strukturerte veiledningen, kapasitetsoppbyggingen og interessentenes engasjement vei for økt digital

sikkerhet på lang sikt. Det endelige målet er å bringe alle skoler opp til standarden innen 2027, under et juridisk rammeverk som er under utvikling hos utdanningsdepartement. Denne historien fungerer som en modell for koordinering på nasjonalt nivå, forhandlingskraft i offentlig sektor og støtte til gjennomføring nedenfra og opp.



Delfinansiert av  
Den europeiske union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.