

# Diving deep into cybersecurity: supporting schools' data privacy and ownership

EXECUTIVE SUMMARY

30 June 2025

## Problem and context

As Dutch schools increase their reliance on digital learning tools and EdTech services, data privacy and cybersecurity have emerged as critical concerns. However, schools often lack the expertise, time or standardised processes to manage these risks effectively. A decentralised education system, where school boards act independently, compounds this issue by creating variability in digital safety maturity across institutions.

In response, SIVON, supported by Kennisnet and the Dutch Ministry of Education, initiated a series of national measures to strengthen data governance and cybersecurity in primary and secondary education. One such initiative, the Deep Dive project, was launched to assess current digital safety practices and help schools build customised improvement plans.

## The Deep Dive project

The Deep Dive project, conducted by SIVON, evaluated the information security maturity of 15 school boards (representing 290 schools and 80 000 students), using a newly developed [Framework of Standards](#) comprising 69 benchmarks across 15 domains (e.g., risk management, security policy, incident handling). Key steps included:

1. **Baseline assessment.** Certified auditors spent two days evaluating each school board's data privacy infrastructure and rated them on a 1–4 maturity scale. Schools scored between 1.3 and 2.5, indicating lots of differences between schools.
2. **Customised improvement plans.** Findings were discussed with relevant stakeholders (school leaders, ICT staff, HR), and tailored recommendations were provided. Schools received risk summaries and committed to specific actions based on their needs and maturity level.
3. **Training and capacity building.** Schools were encouraged to train staff, define roles in digital safety, visualise ICT environments, and develop policies for email and file storage protocols.
4. **Case example – De Rank.** This primary school collaborated with SIVON to develop a data safety action plan, promote ICT training, and improve digital infrastructure mapping and responsibility allocation.

Beyond the Deep Dive, SIVON and Kennisnet offered a **comprehensive suite of services** to enhance school-wide digital safety.

- **Bulk purchasing** of EdTech tools, services and infrastructure at reduced costs. For instance this helped negotiating prices, in one case, a reduction of 40% for interactive white boards.
- **Model privacy agreements** to streamline legal compliance.
- **Emergency response units** for malware or ransomware incidents.

- **Professional networks** like the 900-member “Network IBP” to share practices.
- **Risk analysis services** and practical guidelines for implementing cybersecurity policies.

In parallel, **nationwide negotiations with tech giants (e.g., Google, Microsoft, Apple)** led to critical gains such as data ownership guarantees and limits on commercial data use. These negotiations were informed by **data protection impact assessments (DPIAs)** led by SIVON.

## Lessons learned

- Areas of organisation, risk management and system development were consistently weak. A common issue is that schools don't have a crisis management plan and strong data backup practices. They also do not have descriptions of tasks regarding data safety. The most common need of schools at an initial look are to increase knowledge of data safety, centralising the management of software-as-a-service suppliers and more guidelines.
- Schools are more mature in terms of incident management, because many schoolboards outsource their data protection processes to professional service providers.
- Most schools fell short of meeting baseline standards. Smaller schools in particular struggled due to limited capacity.
- Schools tend to prioritise the functionality of tools over privacy safeguards, such as how personal data is stored or processed.
- Schools requested clearer language and more relevant benchmarks from SIVON, especially for those not developing their own software. Centralised supplier risk management was also suggested as more feasible than board-level efforts.
- Trust-based, offline networking events can encourage transparency from less mature schools and foster productive exchange of best practices.
- The initial sample skewed toward schools already interested in or working on digital safety. Nonetheless, covering 290 schools made this a large-scale and informative pilot for SIVON.

By combining regulatory frameworks, practical tools, centralised negotiations and school-level support, this Dutch model shows how education systems can take meaningful steps to protect school data and make purchase agreements that are more advantageous for schools.

Although the initial evaluations showed considerable room for improvement, the structured guidance, capacity building and stakeholder engagement set the stage for long-term digital safety maturity. The ultimate goal is to bring all schools up to standard by 2027, under a legal framework currently under development by the Ministry of Education. This story serves as a model for national-level coordination, public-sector negotiation power and bottom-up implementation support.



**Co-funded by  
the European 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.