Reactie op het besluit 'Vrij en Veilig Onderwijs'

Het besluit *Vrij en Veilig Onderwijs* brengt aanzienlijke privacyrisico's met zich mee. Als gevolg van dit besluit moeten scholen mogelijk veel meer bijzondere en gevoelige persoonsgegevens verwerken en doorsturen naar de Inspectie van het Onderwijs dan nu het geval is.

De Algemene Verordening Gegevensbescherming (AVG) stelt dat bij de verwerking van persoonsgegevens moet worden voldaan aan de beginselen van proportionaliteit en subsidiariteit. Aan beide vereisten wordt niet voldaan. De toelichting op het besluit vermeldt geen dwingende noodzaak, anders dan de aanname dat scholen onvoldoende inzicht zouden hebben in de oorzaken van eventuele onveiligheid. De Veiligheidsmonitor 2021-2022 laat echter zien dat de meeste leerlingen en personeelsleden zich veilig voelen op school (*zie ook: Een veilig schoolklimaat voor iedereen*). Er is daarom geen rechtvaardiging voor de verwerking van de persoonsgegevens zoals het besluit beoogt.

Daarnaast wordt de verantwoordelijkheid volledig bij de scholen neergelegd. Dit is in strijd met de AVG, waarin is vastgelegd dat degene die het doel en de middelen van de verwerking bepaalt, als verwerkingsverantwoordelijke wordt aangemerkt. In dit geval is dat de overheid.

De reactie van de PO-Raad en VO-Raad op dit besluit wordt door ons volledig onderschreven.

Risico's voor gegevensveiligheid en het beoogde doel

Naast de juridische bezwaren brengt dit besluit ook ernstige risico's met zich mee voor de beveiliging van persoonsgegevens. De digitale dreiging is groot en divers, zoals ook blijkt uit het rapport van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV): Cybersecuritybeeld Nederland 2024.

Gezien deze dreiging is het onverantwoord om meer bijzondere persoonsgegevens van leerlingen en medewerkers te verwerken dan nu gebeurt. Het doel van de monitor is om inzicht te krijgen in de veiligheidsbeleving van leerlingen en medewerkers. Paradoxaal genoeg leidt dit besluit er juist toe dat die veiligheid wordt aangetast.

Hoewel wordt vermeld dat de gegevens gepseudonimiseerd worden, blijft dit een omkeerbaar proces. Door technologische ontwikkelingen wordt het steeds gemakkelijker om gepseudonimiseerde gegevens te herleiden tot individuen.

Indien een school of de leverancier van de monitor wordt getroffen door een cyberaanval en deze gegevens op straat komen te liggen, zijn de gevolgen voor de betrokkenen en de scholen niet te overzien. De kans op dergelijke incidenten is reëel, gezien de toename van cybercriminaliteit in de afgelopen jaren. Het verzamelen van gedetailleerde gegevens maakt scholen bovendien een aantrekkelijker doelwit voor cybercriminelen.

De huidige naleving van het IBP-normenkader (Informatiebeveiliging en Privacy) binnen het primair en voortgezet onderwijs laat zien dat veel scholen niet in staat zijn om persoonsgegevens adequaat te beveiligen.

Conclusie

Het doorvoeren van dit besluit is onverantwoord en vormt een grote bedreiging voor de veiligheid van leerlingen en medewerkers. De titel van het besluit staat haaks op de daadwerkelijke gevolgen ervan.

Bovendien kan dit besluit betekenen dat het onderwijs aan dezelfde strenge eisen voor informatieveiligheid moet voldoen als de zorgsector, waaronder de normen NEN 7510 (informatiebeveiliging) en NEN 7512 (beveiligde communicatie). Dit legt een zware last op scholen, die daar onvoldoende middelen en expertise voor hebben.

We roepen de overheid op om af te zien van de voorgestelde wijzigingen en in plaats daarvan te investeren in maatregelen die de veiligheid op scholen daadwerkelijk bevorderen, zonder de privacy en gegevensbescherming van leerlingen en medewerkers in gevaar te brengen.