Update rapportage verbetermaatregelen DPIA Esis-Rovict
versie 1.0, december 2022

Inleiding

In 2021 is een DPIA (Rapportage DPIA - Esis v1.1) uitgevoerd op het leerlingadministratiesysteem Esis. In de DPIA wordt aanbevolen om risico-beperkende beheersmaatregelen uit te voeren om de aangetroffen privacyrisico's te beperken. De mitigerende maatregelen bestaan uit organisatorische maatregelen bij de school, maatregelen m.b.t. de inrichting van de dienst en tot slot maatregelen vanuit de leverancier van de dienst. Dit document beschrijft een update van de genomen en te nemen maatregelen van Esis – leverancier Rovict - om de benoemde risico's in de DPIA te mitigeren.

SIVON is voornemens om de uitgevoerde DPIA's op de leerlingadministratiesystemen te herhalen. Hierbij wordt de systematiek gevolgd van de DPIA's op de systemen van Microsoft, Google en personeelsadministratiesystemen. De uitkomsten van de eerdere DPIA worden daarin meegenomen.

Hoe is onderstaande tabel tot stand gekomen

In het Esis DPIA rapport zijn een set maatregelen benoemd om de risico's te beperken. De maatregelen die de leverancier (=verwerker) genomen heeft staan in onderstaande tabel. In de kolom "maatregel verwerker" staan de maatregelen van Esis. De kolom "status" geeft aan of deze maatregel voldoende is.

Conclusie

Een aantal van de constateerde hoge risico's zijn door de leverancier gemitigeerd, een aantal risico's moeten door het schoolbestuur worden beperkt door het nemen van (aanvullende) organisatorische maatregelen. We adviseren schoolbesturen aansluiting te zoeken bij de klankbordgroep Management en ICT van Rovict.

Risico nummer	Risico	Risico waardering	Risico beschrijving	Maatregel verwerker	Status
5.1.1	Persoonsgegevens worden opgeschoond volgens het vastgestelde beleid voor bewaren en opschonen (AVG art. 5).	Hoog	Het is voor Verwerkingsverantwoordelijke mogelijk om gegevens in de applicatie op te schonen conform de wettelijke bewaarplicht en/of richtlijnen.	Het is niet mogelijk om aan bepaalde data een bewaartermijn te koppelen. Wel zorgt Rovict 2x per jaar voor een “clean sweep”. Waarbij verouderde data verwijderd wordt.	Schoolbesturen zullen interne beleidsmaatregelen moeten treffen om persoonsgegevens volgende geldende bewaartermijnen te verwijderen.
5.4.1.	Regelmatig behoort een back-up (kopie) van gegevens te worden gemaakt (ISO 12.3.1)	Zeer laag	Er wordt periodiek (op basis van classificatie) een kopie van de gegevens in de applicatie gemaakt middels een beveiligde opslag. Er is een procedure om in het geval van DDOS aanvallen de continuïteit te borgen.	Rovist maakt 2x per dag een back-up. Rovict voldoet aan de Edustandaard m.b.t. BIV (2,2,3) classificatie. De RPO & RTO bedraagt max 24 uur. De back-up wordt periodiek getest.	Geen rest risico
5.5.1.	Er mogen niet meer persoonsgegevens worden uitgewisseld via geautomatiseerde koppelingen dan strikt noodzakelijk en alleen op basis van grondslag en doelbinding (AVG art. 5, 6, 25).	Zeer hoog	Geautomatiseerde koppelingen kunnen in het LAS door of op verzoek van het schoolbestuur ingezien en zo nodig gewijzigd worden op basis van noodzakelijkheid, grondslag en doelbinding.	Elke automatische koppeling moet handmatig geactiveerd worden. Hierbij zit een beschrijving van de gegevens-set die wordt uitgewisseld en dus heeft de gebruiker zicht op de betreffende set gegevens. Rovict conformeert zich aan landelijke standaarden. Deze standaarden zijn getoetst op grondslag en doelbinding vb. UWLR-standaard. Rovict neemt daarbij actief deel aan de verdere ontwikkelingen van dergelijke standaarden en ketenafspraken in de daarvoor opgezette werkgroepen	Geen rest risico

				onder aansturing van EDU-K en Edustandaard.	
5.5.2	Het maken van handmatige exports van persoonsgegevens is niet toegestaan, zonder voldoende waarborgen voor de bescherming van de persoonsgegevens (AVG art. 32).	Hoog	Persoonsgegevens worden (bij voorkeur) vanuit het LAS uitgewisseld via beveiligde geautomatiseerde koppelingen in plaats van handmatige exports. Indien persoonsgegevens (toch) handmatig worden geëxporteerd, dan wordt hiervan een logging bijgehouden. Middels autorisaties is te bepalen welke functies een export kunnen maken. Persoonsgegevens kunnen vanuit het LAS worden uitgewisseld via een mailvoorziening die voldoet aan de standaarden voor beveiligd mailen (NTA7516 en/of 'UBV Veilig en Betrouwbaar e-mailverkeer').	Over de huidige mail functionaliteit zal in samenspraak met onze verschillende klankbordgroepen vastgesteld worden in hoeverre deze nog gewenst is.	Schoolbesturen moeten beleid vaststellen voor het maken van exports. Schoolbesturen moeten uitwisseling van gegevens via mail lokaal beoordelen. Kernvraag daarbij is welke gegevens via de mailvoorziening uitgewisseld wordt.
5.5.3	Het downloaden van bestanden met persoonsgegevens uit het LAS wordt beperkt (AVG art. 5, 32).	Hoog	Bestanden (extern) met persoonsgegevens kunnen vanuit de applicatie worden ingezien waardoor het downloaden hiervan wordt beperkt of geheel niet nodig is.	Het lokaal downloaden van bestanden zal verminderen doordat een pdf-viewer beschikbaar is in ESIS.	Schoolbesturen wordt geadviseerd het voorkomen van schaduwadministraties op te nemen in hun ICT beleid.

5.5.4	Er mogen niet meer persoonsgegevens worden geregistreerd dan strikt noodzakelijk (AVG art. 5).	Hoog	Het schoolbestuur moet zelf kunnen bepalen welke velden verplicht ingevuld en/of getoond moeten worden, dit moet niet door het LAS worden bepaald.	Het beschreven risico van het vastleggen van te veel persoonsgegevens en de daarbij bijbehorende maatregel om als schoolbestuur zelf te bepalen welke velden verplicht ingevuld en/of getoond worden, willen wij graag bespreken met de klankbordgroep Management en ICT. Sommige velden waren vroeger relevant, nu niet meer en verdwijnen. Bij enkele andere (vooral bijzondere) velden zou je dit principe goed kunnen toepassen maar veel andere velden worden incidenteel gebruikt of soms worden zaken vastgelegd van een leerling voor een andere verwerker. Hier is de verwerkingsverantwoordelijke leidend in de bepaling of er een grondslag en doelstelling is voor de betreffende verwerking.	Maatregel schoolbestuur – leg niet meer informatie vast dan strikt noodzakelijk.
5.5.5	Geautomatiseerde koppelingen voor de uitwisseling van persoonsgegevens moeten voldoen aan de hiervoor geldende en actuele beveiligingsstandaarden (AVG art. 32).	Zeer laag	Geautomatiseerde koppelingen waarbij er persoonsgegevens worden uitgewisseld voldoen aan de actuele versie van de Edukoppeling transactiesstandaard en het Certificeringsschema.	Esis – Rovict volgt de Edustandaard voor koppelingen. In Edustandaard is de (minimale) dataset die uitgewisseld wordt gespecificeerd.	Geen rest risico