Update rapportage verbetermaatregelen DPIA Magister - Iddink
versie 1.1, oktober 2022

Inleiding

In 2021 is een DPIA (DPIA Magister rapport versie 1.2 juni 2021) uitgevoerd op het leerlingadministratiesysteem Magister. In de DPIA wordt aanbevolen om risico-beperkende beheersmaatregelen uit te voeren om de aangetroffen privacyrisico's te beperken. Hierbij zijn een aantal maatregelen beschreven. 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 de maatregelen van Magister – leverancier Iddink - om de benoemde risico's in de DPIA te mitigeren. In het DPIA rapport van 2021 is de reactie van Magister niet verwerkt. Het kan dus zijn dat de constateringen op de datum van publicatie van de DPIA reeds niet meer van toepassing waren.

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 Magister DPIA rapport zijn een set maatregelen benoemd om de risico's te beperken. De maatregelen die de leverancier (=verwerker) zou moeten nemen naar aanleiding van dit rapport staan in onderstaande tabel. Om deze tabel te maken zijn de risico's uit het oorspronkelijke DPIA rapport geïnventariseerd en alleen hoge(re) risico's overgenomen met openstaande toezegging vanuit de leverancier. Reeds gemitigeerde maatregelen ten tijde van het tot stand komen van het oorspronkelijk DPIA rapport staan niet in onderstaande tabel.

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.

Risico nummer	Risico	Risico waardering	Risico beschrijving	Maatregel verwerker	Status en restrisico

5.5.1	Er mogen niet meer persoonsgegevens worden uitgewisseld dan strikt noodzakelijk en alleen op basis van grondslag en doelbinding (AVG art. 5, 6, 25).	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.	Als onderdeel van het Magister Partner Programma valt onder andere een privacy check op de partner en doelbinding van de gegevensaanvraag. Indien deze aanvraag positief is doorlopen zal de partner worden toegevoegd. Dat is een eerste stap, maar data zal pas worden verstrekt *na toestemming* van u als school. Binnen de Privacy Manager kan een school van elke partner inzien welke gegevens worden verstrekt en consent geven voor de uitwisseling. Op deze manier heeft u als school controle over de uitwisseling. De Privacy Manager is momenteel operationeel en beschikbaar voor alle scholen.	Met Privacy Manager hebben scholen volledige controle over uitwisseling van gegevens. Er resteert dan geen risico, de school heeft controle over de uitwisseling van gegevens.
5.5.3	Het downloaden van bestanden met persoonsgegevens uit het LAS wordt beperkt (AVG art. 5, 32).	Zeer Hoog	Bestanden met persoonsgegevens kunnen vanuit de applicatie alleen worden ingezien en/of gedownload door medewerkers die daarvoor geautoriseerd zijn.	Exports en downloads zijn beperkt mogelijk in Magister en veelal voorzien van aparte autorisatie (een 'recht') zodat toegang beperkt kan worden. Voor bepaalde functies binnen Magister, zoals het zorgdossier OPP, is het downloaden een extra recht dat specifiek moet worden toegekend aan een gebruiker. Wij onderzoeken als onderdeel van onze voortdurende toetsing waar deze extra autorisatie nog meer moet worden doorgevoerd. Vanaf schooljaar 2022/2023 zijn voor het downloaden en exporteren rechten voor Magister Web OP en OOP in te stellen.	Voor het downloaden en exporteren zijn aparte rechten in te stellen voor de OOP-versie van Magister. Voor OP zijn deze rechten vanaf schooljaar 2022/2023 ook in te stellen. Hiermee wordt het downloaden van gegevens beperkt. Zorg voor juiste instellingen, afspraken en beleid over het gebruik van de exports en downloads, en beperk daarmee het risico tot midden.

					Bepaal of er voor uw organisatie nog (andere) rest-risico's zijn op basis van deze informatie.
5.5.5	Bijzondere of gevoelige persoonsgegeve ns worden beveiligd gemaild (AVG art. 32).	Zeer Hoog	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').	De communicatie functionaliteiten van Magister, e-mail en Berichten, zijn bedoeld om te communiceren naar de bij de school betrokken actoren; OOP-ers, docenten, leerlingen en ouders/verzorgers. Het is niet mogelijk om vanuit Magister een e-mail te versturen naar personen buiten deze 'Magister kring'. Ons advies is altijd om *geen* persoonsgegevens te versturen, maar om gebruikers erop te wijzen dat ze naar hun Magister-omgeving te gaan om daarin zaken te raadplegen. Wij adviseren daarom nadrukkelijk om actief gebruik te maken van leerling- en ouder-accounts zodat ouders zelf gegevens kunnen inzien in de veilige Magister omgeving en dit niet hoeft te worden gemaild naar ze. Magister volgt de richtlijnen en standaarden die bij het onderwijs wordt afgesproken binnen het EDU-K Momenteel vindt er onderzoek plaats binnen Edu-K naar de invoering van een 'veilig mailen protocol' binnen het onderwijs. Er zijn nieuwe richtlijnen veilig mailen (versie 1.0) https://www.edustandaard.nl/standaard_afspraken/ubv-veilig-en-betrouwbaar-e-	Het emailen is beperkt tot gebruikers die bekend zijn in Magister. Zorg als school voor beleidsmaatregelen om ongeoorloofde of ongecontroleerde uitwisseling van bijzondere persoonsgegevens te voorkomen. Zorg voor ouders- en leerlingaccounts i.p.v. mailen van persoonsgegevens. Deel deze afspraken met medewerkers en zorg voor heldere gebruiksinstructies. Met het juiste beleid en afspraken wordt het risico beperkt tot midden of laag. Bij implementeren van standaarden voor veilig mailen worden de risico's verder beperkt.

				mailverkeer/ubv-veilig-en-betrouwbaar-e-mailverkeer-v1-0/ Magister onderzoekt momenteel de nieuwe richtlijnen voor veilig mailen.	
5.5.6	Er mogen niet meer persoonsgegevens worden geregistreerd dan strikt noodzakelijk (AVG art. 5).	Hoog	Het schoolbestuur moet zelf kunnen bepalen welke velden verplicht ingevuld moeten worden, dit moet niet door het LAS worden bepaald.	Magister wordt vormgeven in overleg met gebruikers. Op basis hiervan zijn er binnen Magister al mogelijk om in detailvelden verplicht en niet verplicht te stellen. Hierbij wordt ook gekeken naar verantwoording . Maar uiteraard staan we open tot verbeteren.	Het blijft niet mogelijk om individuele velden te (de)selecteren als verplicht of onverplicht als individuele school. Magister biedt de mogelijkheid aan om in overleg met gebruikers de velden vorm te geven. Detailvelden kunnen wel geselecteerd worden als verplicht. Het schoolbestuur blijft hiermee onvoldoende in control. Het risico wordt enigszins beperkt tot midden. Magister zal voortgang op dit onderdeel moeten tonen om risico's verder te beperken nu het hier gaat om de grondbeginselen van de AVG (dataminimalisatie).