Update rapportage verbetermaatregelen DPIA ParnasSys – Topicus
Versie: september 2022

In 2021 is een DPIA (Remediation report op basis van Rapportage DPIA - ParnasSys v1.1) uitgevoerd op het leerlingadministratiesysteem ParnasSys. 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 ParnasSys – leverancier Topicus - om de benoemde risico's in de DPIA te mitigeren. In het DPIA rapport van 2021 is de reactie van ParnasSys 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.

ParnasSys organiseert speciale expertgroepen (met scholen). We adviseren scholen aan te sluiten bij deze expertgroepen.

Hoe is deze tabel tot stand gekomen

In het ParnasSys 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 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 (per 09/22)	Status
5.1.1	Toegang tot persoonsgegevens wordt verleend volgens het vastgestelde toegangsbeveiligingsbeleid (ISO 5.1.1).	Hoog	Het periodiek wijzigen van wachtwoord en/of de complexiteit van het wachtwoord kan niet afgedwongen worden in de applicatie (indien er geen gebruik wordt gemaakt van 2-factor-authentication). Groepsautorisaties kunnen bij bepaalde rollen als 'default setting' ingesteld worden. Er kan op leerlingniveau of onderdelen van een leerling dossier autorisaties ingesteld worden.	ParnasSys gaat op korte termijn geen aanpassingen doorvoeren t.a.v. het periodiek aanpassen van wachtwoorden. Uit diverse studies blijkt juist dat het frequent aanpassen van wachtwoorden juist onveiliger maakt. ParnasSys adviseert daarom gebruik te maken van 2FA. Dit kan middels soft- of hardtokens. Ook kan gebruik worden gemaakt van Google of Microsoft SSO, welke 2FA en het periodiek wijzigen van wachtwoorden kan afdwingen. ParnasSys ondersteunt het verplichten van 2FA door het bestuur aangemerkte gebruikersrollen. Op de roadmap van ParnasSys staat dat op leerling niveau instellen van autorisaties de komende tijd verder geanalyseerd wordt. ParnasSys doet dit in samenwerking met	Bij de risicobeschrijving zijn 3 onderdelen onderscheiden. Parnassys geeft antwoord op het 1e onderdeel. Het advies is om 2FA te implementeren. Groepsautorisaties kunnen bij bepaalde rollen niet als 'default setting' ingesteld worden (denk aan m.n. aan de rol leerkracht). Standaard staat de groepsautorisatie niet aan, dit is niet in lijn met Privacy by default (design). Wel is in te stellen dat deze aangezet worden. Het advies is om groepsautorisaties te gebruiken, schoolbesturen moeten hier de juiste implementatie kiezen. Ten aanzien van het 3e aspect (op leerlingniveau of onderdelen van een leerling dossier autorisaties instellen) is het advies aan te sluiten bij de (adviezen van de) LAS Expertgroep. Met deze maatregelen wordt het risico beperkt.

				onze LAS Expertgroep. Bij een positieve uitkomst zullen wij dit implementeren	
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).	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.	ParnasSys maakt afspraken met koppelpartners over de gegevens welke verwerkt worden in koppelingen. Deze gegevens zijn per koppelpartner om maat in te richten en zijn voor alle afnemers van de koppeling gelijk. Indien er voor een koppeling niet afdoende wordt gefilterd conform de AVG, dan kan ParnasSys in overleg met de afnemers en koppelpartners de gegevensset minimaliseren. Ook kleine uitbreidingen gaan in overleg met de koppelpartner. Scholen / besturen kunnen zelf bepalen of ze de koppeling afnemen en moeten expliciet toestemming geven voordat een koppeling geactiveerd wordt. Bovendien worden zowel scholen als koppelpartners erop gewezen	ParnasSys maakt afspraken met leveranciers over welke gegevens noodzakelijk zijn voor de koppeling, hierbij is zonodig maatwerk mogelijk. Dataminimalisatie is mogelijk. Besturen beslissen zelf over afname van de koppeling en activeren hiervan. Parnassys biedt ook een generieke koppeling aan waarbij niet – vooraf – ingeschat kan worden of en welke data wordt uitgewisseld zodat niet uitgesloten kan worden dat er bovenmatig veel data wordt uitgewisseld. Advies is om deze koppeling daarom niet te gebruiken maar een specifieke koppeling voor iedere specifieke leverancier. Het is hierbij aan het schoolbestuur hier een risicobeoordeling uit te voeren. Bij verder afstemming van koppelingen is de ParnasSys LAS Expertgroep betrokken als

				dat het noodzakelijk is een verwerkersovereenkomst af te sluiten over de verwerking van, via een koppeling van ParnasSys geleverde, data. Voor eventuele verdere afstemming verwijzen we naar de ParnasSys LAS expert groep.	vertegenwoordiger van verwerkingsverantwoordelijken. Met deze maatregel wordt het risico beperkt.
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).	Middel	Persoonsgegevens worden bij voorkeur vanuit het LAS uitgewisseld via beveiligde geautomatiseerde koppelingen in plaats van handmatige exports.	Het is binnen ParnasSys mogelijk om handmatige exports van gegevens te maken, bijvoorbeeld naar Excel. Hierbij is de uitdaging om een goede balans te vinden tot enerzijds de behoefte van eindgebruikers versus bescherming van persoonsgegevens. ParnasSys is een open platform, waarbij het mogelijk is voor (nieuwe) koppelpartners middels een beveiligde verbinding gegevens uit te wisselen. Het streven is om hier zoveel mogelijk gebruik van te maken. ParnasSys adviseert scholen en besturen gebruikers bewust te maken omtrent de gevaren	ParnasSys biedt geen optie om handmatige exports ‘uit te zetten’ Voor het uitwisselen van gegevens wordt geadviseerd om gebruik te maken van koppelingen (en niet exports). Schoolbesturen moeten interne beleidsmaatregelen (organisatorische maatregel) nemen met als strekking het reguleren of verbieden van downloads. Daarmee wordt het intern misbruik in enige mate beperkt. Alle medewerkers moeten kennis (kunnen) nemen van deze instructie. Dit onderdeel blijft een (gemiddeld) risico omdat uitwisselingen mogelijk blijven waarop de

				van handmatige exports. Ditzelfde geldt ook voor het maken van bijvoorbeeld screenshots of het kopiëren/ plakken van gegevens.	verwerkingsverantwoordelijke onvoldoende zicht heeft. De verwerker heeft hier geen technische maatregel die het risico verder beperkt.
5.5.3	Het downloaden van bestanden met persoonsgegevens uit het LAS wordt beperkt (AVG art. 5, 32).	Laag	Bestanden met persoonsgegevens kunnen vanuit de applicatie worden ingezien. Het downloaden hiervan wordt beperkt.	Zie punt 5.5.2. Daarnaast biedt ParnasSys SSO en bestandskoppeling met Sharepoint en Google. Met deze oplossing is het niet nodig om lokaal bestanden op te slaan.	Bij het genereren van overzichten creëert ParnasSys automatisch een bestand in de map downloads. Schoolbesturen moeten interne beleidsmaatregelen (organisatorische maatregel) nemen met als strekking het reguleren of verbieden van downloads. Daarmee wordt het intern misbruik in enige mate beperkt. Alle medewerkers moeten kennis (kunnen) nemen van deze instructie. Het 'niet nodig zijn' om gegevens lokaal op te slaan, kan niet worden beperkt of uitgezet. Dit blijft een risico.
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 moeten worden, dit moet niet door het LAS worden bepaald.	In ParnasSys kunnen van meerdere soorten personen gegevens worden geregistreerd en verwerkt. Voor Leerlingen zijn veel gegevens vereist voor het	ParnasSys heeft een groot aantal verplichte velden (gegevens categorieën) geschrapt zodat er niet meer persoonsgegevens verwerkt (hoeven te) worden dan noodzakelijk. Hiernaast blijft

				adequaat kunnen leveren van goed onderwijs. Voor Ouders is de gegevensset een stuk beperkter en bestaan de verplichte velden uitsluitend uit gegevens die nodig zijn voor het leveren van goed onderwijs aan de kinderen, dan wel voor het communiceren met ouders over deze kinderen. Voor medewerkers heeft ParnasSys het afgelopen jaar veel stappen gezet om de gegevens te minimaliseren. Allereerst is het aantal velden dat als 'verplicht' stond aangemerkt verkleind. Vanaf 10 augustus zal een groot deel van de beschikbare velden geschrapt worden, zodat deze gegevens niet meer verwerkt worden.	het noodzakelijk om binnen de organisatie te bespreken of en welke gegevensvelden worden gebruikt. Het risico is hiermee beperkt.
5.5.5	Geautomatiseerde koppelingen voor de uitwisseling van persoonsgegevens moeten voldoen aan de hiervoor geldende en actuele beveiligingsstandaarden (AVG art. 32).	Laag	Geautomatiseerde koppelingen waarbij er persoonsgegevens worden uitgewisseld voldoen aan de actuele versie van de Edukoppeling transactiesstandaard en het Certificeringsschema.	ParnasSys streeft er naar zoveel mogelijk gegevens uit te wisselen comform de Edukoppeling transactiestandaard en het Certificeringsschema.	Zie ook 5.5.1 ParnasSys maakt afspraken met leveranciers over welke gegevens noodzakelijk zijn voor de koppeling. Dataminimalisatie is hierbij mogelijk. Besturen beslissen zelf over afname van

				Het kan voorkomen dat koppelpartners deze standaard niet ondersteunen. Deze koppelpartners maken dan gebruik van het generiek koppelvlak. Dit koppelvlak is bedoeld voor voorspelbaar en beveiligd transport van vertrouwelijke gegevens tussen twee partijen en voldoet actuele / erkende beveiligingsstandaarden.	de koppeling en activeren hiervan. ParnasSys is bekend met de standaard. Het is aan schoolbesturen om van de te koppelen leveranciers te eisen dat deze aan de in het onderwijs gebezigde standaarden voldoen. Bij verder afstemming van koppelingen is de ParnasSys LAS Expertgroep betrokken als vertegenwoordiger van verwerkingsverantwoordelijken.
5.6.1	Er vinden periodieke controles plaats of het opschonen van persoonsgegevens gebeurt volgens het daarvoor vastgestelde beleid (ISO 18.2.2).	Middel	Inactieve accounts van medewerkers kunnen inzichtelijk gemaakt en opgeschoond worden.	Het controleren of het opschonen van persoonsgegevens is gebeurd is een verantwoordelijkheid van de school / bestuur. Om dit te kunnen controleren bieden we binnen ParnasSys diverse overzichten waarin gebruikers deze gegevens kunnen inzien.	Het controleren van inactieve accounts of opschonen van gegevens is mogelijk aan de hand van overzichten die ParnasSys levert. Dit is echter handwerk zodat de kans op fouten blijft bestaan (los van de omstandigheid dat dit handwerk tijd vraagt waar het in het onderwijs aan ontbreekt). Deze optie voldoet aan een minimale eis maar is weinig gebruiksvriendelijk en laat kans op fouten bestaan.

					Dat ParnasSys dit proces kan verbeteren blijkt uit het inzichtelijk maken en verwijderen van gegevens van inactieve leerlingen. Dit gaat veel eenvoudiger. Een dergelijke aanpak voor medewerkers zou hier op zijn plaats zijn. De maatregel beperkt het risico in enige mate.