

Evaluatie plan van aanpak Privacy, periode januari 2021 tot en met december 2021
Stichting Montessori Onderwijs Zuid-Holland

Dit plan is januari 2021 opgesteld in overleg met de Functionaris gegevensbescherming op basis van de evaluatie van het plan van aanpak van 2020 en de analyse het jaarverslag 2018-2020 (van de vorige Functionaris gegevensbescherming). Op basis van deze gegevens zijn de volgende acties in overleg met het bestuur opgesteld voor kalenderjaar 2021. De prioriteiten zijn geselecteerd op basis van wettelijke verplichtingen, risico afweging en/of op basis van logistiek. Hieronder staat de evaluatie van de gekozen actiepunten.

Maatregel	Evaluatie
<p>Bewaren en opschonen fysieke en digitale persoonsgegevens</p> <ul style="list-style-type: none"> - Implementeren procedure (januari/februari controleren scholen stand van zaken opschonen oude gegevens): afgerond - Herinneren scholen jaarlijks uitvoeren opschonen gegevens (periode juni-oktober) - Controleren met administratief medewerker of OSO-bestand in nieuwe versie van Parnassys bewaard blijft na verwijderen gegevens leerling na 2 jaar: lopend + DPIA Parnassys en handboek Parnassys 	<p>De procedure opschonen data is geïmplementeerd. Scholen hebben de oude gegevens verwijderd periode december 2020-maart 2021. Jaarlijks worden de gegevens opgeschoond (periode juni-oktober). De privacy coördinator brengt dit binnen het MT onder de aandacht en vraagt om terugkoppeling.</p> <p>Procedure opgesteld m.b.t. het verwijderen van gegevens in Parnassys. Dit document moet nog besproken worden in MT. Eerst zal DPIA Parnassys uitgevoerd worden, zodat er aan de procedure nog andere aandachtspunten toegevoegd kunnen worden. Denk aan logging gegevens bekijken, omgaan met invallers en afspraken over aantal applicatiebeheerders op schoolniveau. Het OSO-bestand blijft in de nieuwe versie van Parnassys bewaard na verwijderen van gegevens, maar niet de bijlagen. Hier moet nog een oplossing voor gevonden worden.</p>
<p>Toegangsbeleid</p> <ul style="list-style-type: none"> - Bespreken MT instellen 2FA Parnassys: afgerond - Jaarlijks controleren autorisatiematrix Parnassys (oktober-november) - Parnassys: Controleren hoeveel personen applicatiebeheerder op schoolniveau jaarlijks - Toegangscontrole op HR systeem: lopend - Toegangscontrole op netwerkmappen: lopend, o.a. invoeren 2FA Office 365 	<p>Parnassys 2FA ingesteld per september 2021.</p> <p>Autorisatiematrix Parnassys ingevoerd. Opnemen in jaarplan: jaarlijks controleren periode oktober-november autorisatiematrix Parnassys + aantal applicatiebeheerders op schoolniveau.</p> <p>Netwerkmappen: alle scholen werken met Office 365 onder Azure. Nog niet alle scholen zijn volledig overgestapt naar de cloud, maar dit is een ontwikkeling die we stimuleren. De bestaande lokale servers worden uitgefaseerd. Planning Q1 2022: 2FA invoeren voor Office 365.</p> <p>Q4 hebben we in kaart gebracht hoe de toegangscontrole bij onze HR systemen is geregeld:</p> <ul style="list-style-type: none"> - Youforce is geautoriseerd inclusief rolverdeling. Staat op papier bij Dyade. Elke nieuwe directeur of

	<p>medewerker op bestuursbureau moet aangemeld worden met rol bij Dyade.</p> <ul style="list-style-type: none"> - Camas: Directeuren geautoriseerd voor alleen eigen school. Bestuurslid met portefeuille HR is geautoriseerd voor alle medewerkers MZH. - DDGC: in het document Gesprekkencyclus is de inrichting van DDGC en het gebruik vastgelegd, inclusief rollen en 2FA. <p>Q4 hebben we in kaart gebracht hoe de toegangscontrole bij onze Financiële systemen is geregeld:</p> <ul style="list-style-type: none"> - Voor Exact hebben we 3 gebruikers (medewerkers bestuursbureau) De volgende drie documenten wordt ieder jaar door de accountants gecontroleerd tijdens de interim controle: controlelijst rechten wijziging, controlelijst rechten, overzicht gebruikers en overzicht rollen - Voor ProActive controleert de accountant de volgende overzichten tijdens de interim controle: Medewerkers, Organisatie en Rol geschiedenis - Cogix – Controller is enige beheerder, de directeuren hebben alleen leest recht voor eigen school <p>Aandachtspunt voor 2022 het verstrekken en intrekken van gebruikersaccounts en –devices voor nieuwe en vertrekkende personeelsleden.</p>
<p>ICT</p> <ul style="list-style-type: none"> - Nalopen of alle verwerkersovereenkomsten met ICT-beheerders gecontroleerd zijn: afgerond - ICT risico-analyse meenemen in audit Privacy op school najaar 2021: afgerond - Encryptie laptops (overleggen met beheerder en MT – bitlocker instellen): lopend 	<ul style="list-style-type: none"> - Alle verwerkersovereenkomsten met ICT-beheerders zijn goed gekeurd door Functionaris gegevensbeschermmer. - Q4 2021: werkgroep bestaande uit privacy coördinator, bovenschoolse ict-er en bestuurder hebben een analyse uitgevoerd op het gebied van ICT. Dit heeft geleid tot een notitie met aandachtspunten, die worden meegenomen in het plan van aanpak 2022: encryptie voor devices (dit is nog niet voor alle scholen geregeld), login controles, procesafspraken m.b.t. aanschaffen nieuwe software. - Audit privacy is uitgevoerd Q4: conclusie is dat MZH goed op weg en in voldoende mate in controle is. Aandachtspunten worden meegenomen in plan van aanpak 2022.
<p>Online dataregister</p> <ul style="list-style-type: none"> - Eventuele nieuwe verwerkersovereenkomsten laten beoordelen, indien nodig DPIA uitvoeren: lopend 	<ul style="list-style-type: none"> - In 2021 veel nieuwe verwerkersovereenkomsten laten beoordelen en ingevoerd in online dataregister. Er hoefden hiervoor geen DPIA's uitgevoerd te worden. - Er is een overzicht van de applicaties van de IS. Er is een verwerkersovereenkomst afgesloten met GL education. Er lopen nog onderhandelingen met 2

<ul style="list-style-type: none"> - Nieuwe verwerkersovereenkomsten toevoegen aan online register: lopend - Zicht op de applicaties IS en de persoonsgegevens die daarin verwerkt worden, waar nodig afsluiten verwerkersovereenkomsten en invoeren: lopend 	<p>verwerkers om te komen tot een goede overeenkomst. In de tussentijd worden er een minimum aan privacygevoelige data in deze systemen opgeslagen, denk aan werken met alias en fictieve geboortedatum.</p> <ul style="list-style-type: none"> - Opnemen plan van aanpak 2022: DPIA Parnassys en Google op basis van landelijk format
<p>Blijvende aandacht voor Awareness (privacy berichten alle medewerkers 5x per jaar): lopend</p>	<ul style="list-style-type: none"> - Privacyberichten uitgezet in MZH app: bewaartermijnen in het onderwijs, phishingmails, veilig delen, veilig werken met google. - Informatie aan directeuren gegeven m.b.t. Coronaregistratie. - Vragen van scholen beantwoord. - Vanuit audit: medewerkers zijn goed op de hoogte hoe ze dienen om te gaan met beeldmateriaal en waar ze met vragen over privacy terecht kunnen. Veel medewerkers zijn nog onvoldoende op de hoogte van het handboek en de procedures/regels. Plan van aanpak 2022: Revisie handboek en opslaan centrale plaats
<p>Up to date houden van handboek en bijlagen: lopend</p>	<p>Nieuwe documenten toegevoegd aan handboek: privacyverklaring, autorisatiematrix Parnassys, procedure opschonen data.</p> <p>Opnemen plan van aanpak 2022 n.a.v. audit 2022: Revisie handboek splitsing informatie medewerkers en directie.</p>
<p>Communicatie:</p> <ul style="list-style-type: none"> • Nieuwe privacyverklaring (plaatsen op websites en schoolgids): lopend • Bij vernieuwen websites 'cookie' waarschuwing laten instellen: lopend 	<ul style="list-style-type: none"> - Nieuwe websites zijn in de lucht. Privacyverklaring is opgenomen. Bij controle bleek dat dit een verkorte versie is. Laten aanpassen Q1 2022 - Cookie waarschuwing is ingesteld, echter bij controle bleek dat deze melding niet conform de AVG is. Toestemming moet vrijelijk kunnen worden gegeven, bezoekers optie geven tussen functionele en andere cookies. Laten aanpassen Q1 2022.
<p>Extra acties, die niet opgenomen stonden in plan van aanpak 2021</p>	<ul style="list-style-type: none"> - Naar aanleiding van de ontwikkelingen m.b.t. privacy risico's Google zijn scholen geïnformeerd over de risico's. We hebben de nieuwe overeenkomst afgesloten en scholen hebben de technische maatregelen van checklist zo veel mogelijk doorgevoerd. Q1 2022 DPIA uitvoeren om te zien of de risico's voldoende afgedekt zijn. - 2 datalek meldingen inclusief melding bij AP.