Procedure Toekennen Autorisaties

Stappenplan aangeleverd door Lumen Group in de naleving van de wettelijke verplichting Dataminimalisatie uit de AVG (Artikel 5 lid 1 sub c AVG)

Versie	V1.0
Auteur	Lumen Group
Opsteldatum	17 oktober 202217 oktober 2022

LUMEN GROUP privacy & data

Inhoud

LUMEN GROUP privacy & data

1. Over Autorisaties

1.1 Wat is een autorisatiematrix?

Een autorisatiematrix is een overzicht welke functies binnen en buiten de organisatie toegang hebben tot welke persoonsgegevens[1]. Van de gegevens in het leerlingensysteem, de achterkant van de website, de dagelijkse documenten op de Cloud service tot aan de financiële gegevens in het salarissysteem. Ook kan er een autorisatiematrix worden aangelegd over toegang tot bepaalde fysieke ruimtes of fysieke dossiers.

In een autorisatiematrix wordt vastgelegd welke personen welke rechten binnen bepaalde systemen hebben[2]. Dit wordt eventueel aangevuld met afzonderlijke rechten binnen dat systeem. Het uitgangspunt moet zijn dat niet alle rollen toegang hebben tot alle digitale gegevens. Een leerkracht/docent die alleen werkzaam is in klas 3A mag daardoor alleen toegang hebben tot de gegevens van de leerlingen in klas 3A en niet standaard tot de gegevens van alle leerlingen. Een leerkracht/docent heeft slechts bepaalde persoonsgegevens van leerlingen nodig met als doel het kunnen geven van onderwijs. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd. Hierbij wordt gekeken naar wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien, wijzigen of verwijderen.
Meestal is de autorisatiematrix opgenomen als bijlage bij het informatiebeveiligingsbeleidsplan.

1.2 Waarom een autorisatiematrix?

Scholen hebben op basis van wetgeving en verwerkersovereenkomsten toegang tot veel persoonsgegevens van leerlingen. Deze wetgeving, maar ook de AVG, normen in de Informatiebeveiliging en overeenkomsten stellen eisen aan de maatregelen die scholen dienen te implementeren. Dit om aan te tonen dat de organisatie de belangrijkste risico's binnen haar processen beheerst. Logische toegangsbeveiliging is vaak een van de beheersmaatregelen waar een school op steunt. Een school moet dan ook kunnen aantonen dat de toegangsrechten in een informatiesysteem tijdig en juist zijn geïmplementeerd. Zo dient er geen gebruik gemaakt te worden van ongepersonaliseerde accounts en dienen gebruikers over niet meer rechten te beschikken dan zij voor hun werkzaamheden nodig hebben. Dit wordt ook wel het "Need to Know"-principe genoemd.

Het gebruik maken van gepersonaliseerde accounts en geen 'algemene' identiteiten zorgt ook voor onweerlegbaarheid, herleidbaarheid en transparantie. Hiervoor is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd. Transparantie is de mate van openheid, zichtbaarheid en toegankelijkheid van school naar haar leerlingen en (keten)partners. Dat leidt ertoe dat scholen achteraf in staat zijn verantwoording af te leggen over hun bedrijfsvoering. Intern is dit met name het

[1] AVG: Artikel 5 *(Beginselen inzake verwerking van persoonsgegevens)*, Artikel 6 *(rechtmatigheid van verwerking)* Artikel 24 *(verantwoordelijkheid van de verwerkingsverantwoordelijke)* Artikel 25 *(gegevensbescherming door ontwerp en door standaardinstellingen)* Artikel 32 *(beveiliging van de verwerking)*
[2] AVG Artikel 5 lid 1 sub c *(Dataminimalisatie)*: 1. Gebruik alleen die persoonsgegevens die noodzakelijk zijn om het vastgestelde doel te bereiken. 2. Kijk of je met minder of bijvoorbeeld anonieme gegevens kunt werken. 3. Bewaar de gegevens niet langer dan nodig of dan wettelijk bepaald is.

geval bij datalekken; dan is het handig om te kunnen achterhalen bij welke persoon er in welk systeem een fout ontstaat.
In het geval er niet specifiek genoeg geautoriseerd kan worden: zorg dan dat de logging van het systeem op orde is, zodat achteraf aangetoond kan worden wie wanneer in welk systeem toegang heeft gehad tot persoonsgegevens.

Een goed ingerichte en logische toegangsbeveiliging[3] stelt organisaties in staat om medewerkers de juiste toegang te geven tot de benodigde gegevensverwerkende systemen, of om de toegang van medewerkers weer in te trekken. Goed ingericht gebruikersbeheer leidt ertoe dat autorisaties accuraat worden afgehandeld, waardoor oneigenlijk gebruik zoveel mogelijk wordt tegen gegaan.

Ook kunnen er kostenbesparingen plaatsvinden zowel in de primaire bedrijfsprocessen als in de ondersteunende diensten. Bij een goede logische toegangsbeveiliging kunnen medewerkers eerder aan de slag door een snellere afhandeling van wijzigingsverzoeken bij het gebruikersbeheer. De tweede besparing vindt plaats in de gebruikersbeheerprocessen: door deze efficiënt in te richten zijn minder handelingen nodig van de medewerkers, waardoor de totale kosten van het gebruikersbeheer afnemen.

Kortom, met een autorisatiematrix voldoe je aan de basisprincipes die de AVG voorschrijft:

- Aantoonbaarheid van autorisaties
- Dataminimalisatie
- Inzicht in de risico's van gegevensverwerking
- Leidraad bij incidenten/verzoeken van betrokkenen
- Privacy by design en privacy by default

[3] - Een voorbeeld van niet goed gegeven autorisaties is: GGD medewerkers konden gegevens inzien en verkopen.
- De Autoriteit Persoonsgegevens heeft in 2018 bij diverse scholen in het openbaar (speciaal) basisonderwijs, voortgezet onderwijs en (voortgezet) speciaal onderwijs onderzoeken uitgevoerd naar de autorisaties in hun leerlingvolgsysteem. De AP roept scholen op hun werkwijze met deze systemen tegen het licht te houden. Meer informatie is op de site van de AP te vinden.

2. Hoe maak ik een autorisatiematrix?

2.1 Beleid, rollen en verantwoordelijkheden

Het organiseren van een autorisatiematrix begint met het scheppen van de juiste randvoorwaarden. Dit zal zowel moeten in de vorm van een beleid als in het vastleggen van verantwoordelijkheden. Het organiseren van informatiebeveiliging en privacy op school begint met een Informatiebeveiligings- en Privacybeleid (IBP). Hierin wordt vastgelegd welke uitgangspunten worden gehanteerd bij het beveiligen van informatie en het garanderen van privacy van medewerkers en leerlingen. Ook wordt hierin beschreven welke maatregelen, procedures en afspraken hierbij horen. Beschrijf ook wie de autorisatiematrix beheert, wat de toekenningsprocedure voor nieuwe autorisaties is en wie deze goedkeurt en controleert.

Inventariseer het huidige IT-landschap en de gebruikte fysieke locaties van je organisatie. Inventariseer wie toegang heeft tot welke interne en externe systemen en hoe deze toegang is geregeld/vastgelegd. Een Identity & Access Management-tool (IAM-tool) kan hierbij helpen. Dergelijke tools zien op processen binnen een organisatie die zich richten op het beheren van gebruikers en resources in het netwerk. Het vastleggen van de inventarisatie is niet alleen van belang voor het verwerkingsregister persoonsgegevens, maar kan bij een juiste implementatie ook gebruikt worden als blauwdruk voor verder beheer.

Noteer de lijst met actuele functiebeschrijvingen en orden deze per groep aan de hand van de (persoons)gegevens die deze groep nodig heeft voor de uitoefening van de functie.
Beschrijf hierbij ook de gegevens die de rol '*invaller*' of '*tijdelijke kracht*' nodig heeft tijdens de werkzaamheden. Hierbij kan gedacht worden aan een algemeen account per klas of leerjaar welke tijdelijk open gezet kan worden als deze invaller of tijdelijke kracht de werkzaamheden verricht. Houd een log bij wie wanneer toegang had tot dit account.

2.2 Inventariseer en beperk de risico's

Om persoonsgegevens goed te beveiligen, moet er een overzicht zijn van risico's en bijbehorende beperkende maatregelen. Met een dergelijke risicoanalyse wordt in kaart gebracht over welke persoonsgegevens de organisatie beschikt, waarom en waartegen deze beschermd moeten worden. Zo kunnen de juiste beveiligingsmaatregelen genomen worden. Bij verwerking van persoonsgegevens is het van belang extra aandacht te schenken aan systemen waar bijzondere persoonsgegevens in worden verwerkt als BSN en gezondheidsgegevens.

In de praktijk komt dit neer op het kijken naar het verwerkingsregister en de persoonsgegevens te classificeren met de BIV-classificaties (beschikbaarheid, integriteit en vertrouwelijkheid). Aan de hand van deze classificatie wordt beoordeeld welke mate van beveiliging er per applicatie op persoonsgegevens moet worden toegepast.

2.3 Stel de autorisatiematrix vast

In een autorisatiematrix wordt vervolgens centraal vastgelegd welke rechten aan een gebruiker, gebruikersrol of gebruikersgroep worden toegekend in soorten bestanden. Later wordt dit gesplitst

naar toegangsrechten per applicatie.

Zet in een Excel-bestand:

- Op de X-as de gebruiker, gebruikersrol of gebruikersgroep;
- Op de Y-as een beschrijving van de persoonsgegevens en;
- Per functie bij ieder persoonsgegeven vervolgens een van de volgende rechten:
    - Leesrechten van gegevens
    - Leesrechten van gegevens met extra beveiliging (als BSN, gezondheidsgegevens)
    - Aanmaken en wijzigen van gegevens
    - Verwijderen van gegevens
    - Uitvoeren van specifieke functies (beheerdersaccount, dit kan per applicatie of algemeen zijn)

Veelal zal het erop neerkomen dat je gebruikersgroepen maakt en de bestaande rechten opnieuw toewijst.

Lumen Group heeft hiervoor een Template Autorisatiematrix beschikbaar gesteld, welke als bijlage geldt van dit document.

Met opmerkingen [FP1]: LG eerst noemen, hyperlink naar ons template toevoegen als 'ie op de Kennisbank staat.

2.4 Toets de huidige situatie aan de gewenste situatie – ist vs soll

Toets samen met de functioneel beheerder of er hiaten in de opgestelde matrix zitten. In sommige situaties zal de gewenste situatie namelijk niet met de huidige situatie overeenkomen. Gebruikers hebben vaak meer rechten dan voor de uitoefening van hun functie nodig is. Ga na of de huidige gebruikers bij beperking van hun rechten hun gebruikelijke werkzaamheden nog kunnen uitvoeren en waar de hiaten in de matrix ontstaan.

3. Hoe beheer je een autorisatiematrix?

3.1 Vraag feedback van de functioneel beheerder

Vraag periodiek de functioneel beheerder van het informatiesysteem de autorisaties te controleren en reviewen. Denk hierbij aan het:

- Vaststellen dat periodieke controles zijn uitgevoerd aan de hand van een rapportage en dossiervorming.
- Vaststellen of een medewerker (gebruiker) meerdere gebruikersnamen heeft. Indien dit het geval is, vaststellen dat dit met instemming van de leiding is toegekend en wat de reden is voor twee of meerdere gebruikersnamen. Wellicht is het mogelijk dit te veranderen in het kader van risicobeperkting.
- Vaststellen of alle geautoriseerde medewerkers nog in dienst zijn en/of nog dezelfde functie vervullen als waarvoor men is geautoriseerd.
- Vaststellen of de functiescheiding is doorbroken. Indien dit het geval is, vaststellen dat de functiescheiding bewust is doorbroken en of dit schadelijke gevolgen kan hebben voor bepaalde processen.
- Vaststellen dat gebruikers die meerdere keren toegang tot het informatiesysteem proberen te krijgen, zonder gebruik te maken van de juiste gebruikersnaam en wachtwoord, door het informatiesysteem (al dan niet tijdelijk) zijn geblokkeerd.
- Vaststellen dat periodieke controle van en rapportage over medewerkers met speciale bevoegdheden, die ook bevoegd zijn speciale tools te gebruiken, plaatsvindt.
- Vaststellen dat periodieke controle van en rapportage over ongeautoriseerde logpogingen plaatsvindt.

3.2 Toets de toegewezen indeling aan de realiteit

Toets periodiek of de rechtenindeling ook daadwerkelijk is ingericht in de informatiesystemen en applicaties. Redeneer of de rechten nog wel logisch zijn. Is het nog steeds wenselijk of noodzakelijk dat bepaalde medewerkers of gebruikersrollen bepaalde rechten hebben?

3.3 Rapporteer aan directie

Ga periodiek na welke processen in de praktijk problemen op leveren wat betreft het autorisatiebeheer van de organisatie. Denk hierbij aan: instroom, doorstroom, uitstroom medewerkers of aanschaf nieuwe applicaties. Functioneel beheerders geven in samenspraak met de Privacy Officer periodiek bij het hoogste management aan welke openstaande aanbevelingen er zijn om beslissingen over te nemen. Daarbij worden de volgende zaken meegenomen:

- Een onafhankelijke beoordeling van het ICT beheer over de kwaliteit van uitvoering van de controle is.
- Houden functioneel beheerders van de applicaties zich aan de gewenste volledigheid en tijdigheid van de controle?
- Wat leverde deze controle per functioneel beheerder aan output op?

3.4 Communiceer over wijzigingen richting gebruikers van de systemen

- Houd per matrix de gegeven machtigingsniveaus bij

- Wanneer nieuwe apps in gebruik worden genomen binnen de organisatie, voeg deze dan toe aan de autorisatiematrix.
- Laat iedereen de autorisatiematrix bekijken, bijvoorbeeld via de intranetpagina van het IT-team. Dit zorgt voor transparantie en moedigt aan om deze up-to-date te houden.
- Zorg voor een duidelijk en overzichtelijk proces voor wanneer een gebruiker toegang tot een app wil aanvragen of wijzigen.
- Organiseer trainingen over specifieke apps voor rollen en verantwoordelijkheden in de autorisatiematrix.
- Richt een proces in om autorisaties bij te werken wanneer medewerkers de organisatie verlaten of zich bij de organisatie aansluiten.

3.5 Bewustwording medewerkers

Zorg dat de school specifiek aandacht besteed aan het bewustzijn van medewerkers met betrekking tot het belang van een goede logische toegangsbeveiliging. Dit kan via trainingen en/of door de te nemen acties voor de autorisaties in de PDCA-cyclus voor privacy en informatiebeveiliging en de jaarplanning op te nemen.

Zorg ervoor dat minimaal de volgende punten aan bod komen:

- Toegangscodes en wachtwoorden zijn strikt persoonlijk. Onderlinge uitwisseling is niet toegestaan. Ook aan externe leveranciers worden persoonlijke accounts toegekend met dezelfde restricties.
- Wachtwoorden moeten geheim blijven. Briefjes met daarop het wachtwoord opgeschreven en aan de monitor geplakt zijn niet toegestaan. Overweeg een wachtwoordkluis om wachtwoorden veilig te genereren en op te slaan.
- Medewerkers worden periodiek gewezen op de meest actuele methodes van cybercriminelen om gebruikersnamen en wachtwoorden te achterhalen via bijvoorbeeld spoofing, phishing, shoulder surfing en social engineering .
- Lock je computer als je er (tijdelijk) geen zicht op hebt via Windowstoets + L. Dit voorkomt dat onbevoegden gebruik maken van jouw gebruikersaccount.

3.6 Herhaal periodiek

Herhaal de stappen in het hoofdstuk '*Hoe beheer je een autorisatiematrix*' periodiek zodat de organisatie grip houdt op het autorisatiebeheer. Door deze stappen op te nemen in een dergelijke PDCA-cyclus zal de organisatie in control komen of blijven op het gebied van toegang tot informatie en informatie-verwerkende faciliteiten.

Lumen Group
Lumen Group kan ondersteunen bij het toetsen en implementeren van deze autorisatiematrix. Neem vrijblijvend contact op via fg@lumengroup.nl of 030 889 65 75 om de mogelijkheden te bespreken.

Lumen Group heeft een Template Autorisatiematrix beschikbaar gesteld, welke als bijlage geldt van dit document.

Met opmerkingen [MH|LG2]: Link naar Kennisbank LG toevoegen.

LUMEN GROUP privacy & data

Bijlage: Voorbeeld autorisatie aanvraagformulier <informatiesysteem>

Gegevens gebruiker		
Naam gebruiker		
Gebruiker-ID	<naam/nummer>	
E-mailadres		
Afdeling/Groep		
Functie		
Telefoonnummer		
Duur autorisatie (Tijdelijk/Vast)	Vast / Tijdelijk: aflopend op:	
Autorisatie	**Nieuwe gebruiker**	O
	Wijzig huidige autorisaties	O
	Opschorten gebruiker-ID	O
	Intrekken gebruiker-ID	O
Reden		
Gewenste ingangsdatum		
Einddatum geldigheid	<in geval geen einddatum leeglaten>	

Autorisaties <informatiesysteem>			
Vul de huidige, de gewenste en de te verwijderen autorisatierollen in	**Huidige**	**Verwijderen**	**Nieuwe rol / Toevoegen**
<Rol 1>	O	O	O
<Rol 2>	O	O	O
<Rol 3>	O	O	O
Alle autorisaties verwijderen	O		

Gegevens Aanvrager	
Naam en voorletters aanvrager	
Voornaam aanvrager	
Telefoonnummer	
E-mailadres	
Functie	
Aanmelddatum	
Handtekening	