AUTORITEIT
PERSOONSGEGEVENS

Onderzoeksrapport

Onderzoek naar de toegangsrechten van medewerkers van onderwijsinstellingen van BOOR tot persoonsgegevens van leerlingen in leerlingvolgsysteem X

Rapport definitieve bevindingen

Januari 2018

Rapport definitieve bevindingen
z2016-00234

Inhoudsopgave

1. Inleiding

1.1 Aanleiding onderzoek

Onderwijsinstellingen verwerken veel persoonsgegevens van leerlingen, zoals contactgegevens, burgerservicenummer (bsn), verzuimgegevens, studieresultaten en gegevens over de gezondheid en het welzijn. Zij hebben deze gegevens nodig ter verzorging van het onderwijs aan de leerlingen. Gelet op de aard en omvang van deze persoonsgegevens, waaronder bijzondere persoonsgegevens[1], en het feit dat kinderen zijn aan te merken als kwetsbare personen[2], is het van groot belang dat onderwijsinstellingen zorgvuldig omgaan met de persoonsgegevens en de beginselen van de Wet bescherming persoonsgegevens (Wbp), en vanaf 25 mei 2018 de beginselen van de Algemene verordening gegevensbescherming (AVG), daarbij in acht nemen. De Autoriteit Persoonsgegevens (AP) heeft daarom in haar agenda 2016 aangekondigd dat in het bijzonder aandacht zal worden besteed aan de privacy van kinderen in het onderwijs.[3]

De AP heeft signalen ontvangen over de, mogelijk te ruime, toegangsrechten van medewerkers van onderwijsinstellingen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X (autorisatie). Een risico van een te ruime toegangsverlening is dat medewerkers van een onderwijsinstelling onrechtmatig (bijzondere) persoonsgegevens van leerlingen raadplegen, wijzigen, wissen of verstrekken aan derden. Bovendien zijn de gevolgen van een mogelijk beveiligingsincident groter. Wanneer een onbevoegde de inlogcodes van een medewerker weet te achterhalen, verkrijgt hij immers toegang tot een grote set aan (bijzondere) persoonsgegevens. Naar aanleiding van de signalen heeft de AP een onderzoek ingesteld.

1.2 Leerlingvolgsysteem X

Systeem X is een webbased leerlingvolgsysteem en leerlingadministratiesysteem. Ruim 5.000 onderwijsinstellingen (ongeveer 900 besturen) hebben systeem X in gebruik.

1.3 Organisatiebeschrijving BOOR

Stichting BOOR (hierna: BOOR) verzorgt het openbaar (speciaal) basisonderwijs, voortgezet onderwijs en (voortgezet) speciaal onderwijs in Rotterdam en omstreken. In totaal zijn er 78 scholen, met ruim 3.500 medewerkers en ongeveer 30.000 leerlingen.[4] BOOR is één van de grootste besturen die leerlingvolgsysteem X in gebruik heeft.

[1] Als bijzondere persoonsgegevens worden onder meer aangemerkt de persoonsgegevens betreffende iemands gezondheid (artikel 16 Wet bescherming persoonsgegevens en artikel 9 Algemene verordening gegevensbescherming) en het bsn (artikel 24 Wet bescherming persoonsgegevens). Onder de Algemene verordening gegevensbescherming wordt het bsn niet meer als bijzonder persoonsgegeven aangemerkt, maar wel als een gevoelig persoonsgegeven waar waarschijnlijk speciale regels voor zullen gelden.
[2] In overweging 75 van de Algemene verordening gegevensbescherming worden kinderen expliciet aangemerkt als kwetsbare personen. Overweging 38 van de Algemene verordening gegevensbescherming wijst erop dat kinderen allicht minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens.
[3] Agenda 2016, p.3 (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/autoriteit_persoonsgegevens_agenda_2016.pdf)
[4] Bron: www.stichtingboor.nl

1.4 Doel onderzoek

Het onderzoek beoogt vast te stellen of BOOR passende beveiligingsmaatregelen ten uitvoer heeft gelegd om de persoonsgegevens van leerlingen in leerlingvolgsysteem X te beveiligen tegen onbevoegde kennisneming, wijziging of verstrekking van de gegevens. Meer specifiek is het onderzoek gericht op (aspecten van) toegangsbeveiliging met betrekking tot persoonsgegevens van leerlingen in leerlingvolgsysteem X.

1.5 Onderzoeksvragen

Aan het onderzoek liggen de volgende vragen ten grondslag:

1. Welke medewerkers van onderwijsinstellingen van BOOR krijgen toegang tot welke persoonsgegevens van welke leerlingen in leerlingvolgsysteem X?
2. Is het noodzakelijk dat deze medewerkers toegang krijgen tot de persoonsgegevens van deze leerlingen?
3. Beschikt BOOR over procedures om medewerkers van haar onderwijsinstellingen toegang te geven tot persoonsgegevens van leerlingen in leerlingvolgsysteem X die zij voor de uitvoering van hun taken nodig hebben?
4. Worden de activiteiten die de medewerkers van onderwijsinstellingen van BOOR uitvoeren met persoonsgegevens van leerlingen in leerlingvolgsysteem X gelogd?
5. Worden de logbestanden periodiek gecontroleerd op indicaties van onrechtmatige toegang van de medewerkers van onderwijsinstellingen van BOOR tot persoonsgegevens van leerlingen in leerlingvolgsysteem X?

1.6 Verloop onderzoek

De AP heeft bij brief van 15 maart 2016 de exploitant van leerlingvolgsysteem X (hierna: de exploitant), verzocht om inlichtingen. De exploitant heeft bij brief van 27 maart 2016 (tevens per e-mail van 1 april 2016) inlichtingen verstrekt.

De AP heeft bij brieven van 9 en 24 mei 2016 de exploitant verzocht om nadere inlichtingen. De exploitant heeft bij brief van 27 mei 2016 (tevens per e-mail van gelijke datum) de inlichtingen verstrekt.

De AP heeft bij brief van 13 juni 2016 BOOR verzocht om inlichtingen. BOOR heeft bij brief van 23 juni 2016 (tevens per e-mail van gelijke datum) verzocht om uitstel van reactie. De AP heeft bij brief van 24 juni 2016 uitstel verleend. BOOR heeft bij brief van 15 juli 2016 (tevens per e-mail van gelijke datum) inlichtingen verstrekt.

De AP heeft bij brief van 26 juli 2016 BOOR verzocht om nadere inlichtingen. BOOR heeft bij brief van 22 augustus 2016 (tevens per e-mail van gelijke datum) inlichtingen verstrekt.

De AP heeft bij brief van 8 november 2016 BOOR verzocht om nadere inlichtingen. BOOR heeft bij brief van 22 november 2016 (tevens per e-mail van gelijke datum) inlichtingen verstrekt.

De AP heeft bij brief van 3 januari 2017 BOOR verzocht om nadere inlichtingen. BOOR heeft bij brief van 20 januari 2017 (tevens per e-mail van gelijke datum) inlichtingen verstrekt.

De AP heeft bij brief van 22 mei 2017 het rapport van voorlopige bevindingen betreffende het uitgevoerde onderzoek toegestuurd. De AP heeft BOOR daarbij in de gelegenheid gesteld om schriftelijk haar reactie op dit rapport te geven. BOOR heeft bij brief van 30 mei 2017 (tevens per e-mail van gelijke datum) verzocht om uitstel van reactie. De AP heeft bij brief van 30 mei 2017 uitstel verleend. BOOR heeft bij brief van 30 juni 2017 (tevens per e-mail van 3 juli 2017) een schriftelijke reactie gegeven op het rapport van voorlopige bevindingen.

De AP heeft bij brief van 17 juli 2017 BOOR verzocht om inlichtingen. BOOR heeft bij brief van 6 september 2017 (tevens per e-mail van gelijke datum) inlichtingen verstrekt.

De AP heeft bij brief van 31 oktober 2017 BOOR verzocht om inlichtingen. BOOR heeft bij brief van 13 november 2017 (tevens per e-mail van 14 november 2017) inlichtingen verstrekt.

De AP heeft per e-mail van 6 december 2017 BOOR verzocht om inlichtingen. BOOR heeft bij brief van 11 december 2017 (tevens per e-mail van gelijke datum) inlichtingen verstrekt.

1.7 Juridisch kader

1.7.1 Verantwoordelijke[5]

Ingevolge artikel 1, sub d, Wbp[6] is de verantwoordelijke de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

De wetsgeschiedenis geeft hierover aan:

> *Het begrip 'verantwoordelijke' knoopt in eerste instantie aan bij de vaststelling van het doel van de verwerking. De vraag is wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel. Tevens is van belang wie beslist over de middelen voor die verwerking: de vraag op welke wijze de gegevensverwerking zal plaatsvinden. De richtlijn gaat ervan uit dat deze bevoegdheden in de regel in dezelfde hand liggen. Is dit niet het geval, dan is er sprake van gezamenlijke verantwoordelijkheid.*
> *(...)*
> *Bij de beantwoording van de vraag wie de verantwoordelijke is, dient enerzijds te worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen, anderzijds – in aanvulling daarop – van een functionele inhoud van het begrip.*[7]

1.7.2 Beveiliging

Artikel 13 Wbp bepaalt dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard

[5] In de AVG aangeduid als 'verwerkingsverantwoordelijke'.
[6] Vanaf 25 mei 2018 artikel 4, lid 7, AVG.
[7] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 55

van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.[8]

De AP (destijds het College bescherming persoonsgegevens) heeft in haar Richtsnoeren beveiliging van persoonsgegevens[9] nader uitgewerkt wat onder 'passende technische en organisatorische beveiligingsmaatregelen' moet worden verstaan. Daarbij is aangesloten op standaarden, methoden en maatregelen die in het vakgebied informatiebeveiliging gebruikelijk zijn.

Voor onderwijsinstellingen is met name de, thans geldende, Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging[10] (hierna: de NEN 27002) van belang. De NEN 27002 is een technologieneutrale standaard die binnen de informatiebeveiliging breed wordt toegepast bij het formuleren en implementeren van beveiligingsmaatregelen. De NEN 27002 is bovendien opgenomen op de 'pas toe of leg uit'-lijst van het College en Forum Standaardisatie. Dit betekent dat (semi-)overheidsorganisaties, waaronder onderwijsinstellingen, de NEN 27002 toe moeten passen of uit moeten leggen waarom ze dat niet doen.

Bij de toetsing van beveiligingsmaatregelen van onderwijsinstellingen aan artikel 13 Wbp gebruikt de AP het bepaalde in haar Richtsnoeren beveiliging van persoonsgegevens en de NEN 27002 als ijkpunt.

[8] Artikel 32, lid 1, AVG bepaalt dat rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treft om een op het risico afgestemde beveiligingsniveau te waarborgen.
[9] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, februari 2013 (https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-richtsnoeren-beveiliging-van-persoonsgegevens)
[10] NEN-ISO/IEC 27002+C1+C2, december 2015. Deze standaard is de opvolger van de Code voor Informatiebeveiliging, NEN-ISO/IEC 27002:2007 nl, die gold ten tijde van de opstelling van de Richtsnoeren beveiliging van persoonsgegevens.

2. Bevindingen

2.1 Uitwerking van het juridisch kader

Ingevolge artikel 13 Wbp dient BOOR passende technische en organisatorische maatregelen ten uitvoer te leggen om de persoonsgegevens van leerlingen in leerlingvolgsysteem X te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Onder onrechtmatige vormen van verwerking vallen onder meer de onbevoegde kennisneming, wijziging of verstrekking van de gegevens.[11]

BOOR dient derhalve (onder andere) beveiligingsmaatregelen te treffen om toegang tot persoonsgegevens van leerlingen in leerlingvolgsysteem X voor bevoegde medewerkers van haar onderwijsinstellingen te bewerkstellingen en onbevoegde toegang tot deze persoonsgegevens te voorkomen.[12] De volgende aspecten van de Richtsnoeren Beveiliging van persoonsgegevens en de NEN 27002 zijn betrokken bij de beoordeling of BOOR passende beveiligingsmaatregen heeft getroffen op het gebied van toegangsverlening aan medewerkers van haar onderwijsinstellingen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X:

- Er dienen procedures te zijn om medewerkers van onderwijsinstellingen van BOOR toegang te geven tot persoonsgegevens van leerlingen in leerlingvolgsysteem X die zij voor de uitvoering van hun taken nodig hebben[13] [14]:
    - Er dient een formele registratie- en afmeldingsprocedure te zijn om toewijzing van de toegangsrechten aan de medewerkers mogelijk te maken[15] alsmede een formele gebruikerstoegangsverleningsprocedure om toegangsrechten voor alle typen gebruikers toe te wijzen of in te trekken[16].
    - Deze procedures dienen te zijn geïmplementeerd.[17]
- Er dienen logbestanden te worden gemaakt van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren.[18]
- De logbestanden dienen regelmatig te worden beoordeeld.[19]

2.2 Feitelijke bevindingen

2.2.1 Persoonsgegevens van leerlingen in leerlingvolgsysteem X

BOOR heeft in haar brief van 15 juli 2016 aangegeven dat de volgende persoonsgegevens van leerlingen haar onderwijstellingen in leerlingvolgsysteem X worden verwerkt:

[11] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 98. Artikel 32, lid 2, AVG noemt onder meer de ongeoorloofde verstrekking van en ongeoorloofde toegang tot opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
[12] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 9.2 NEN 27002
[13] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 9.2 NEN 27002
[14] Dit betekent dat er grenzen dienen te worden gesteld aan de kring van medewerkers die toegang verkrijgen tot persoonsgegevens van leerlingen. Ook dienen er grenzen te worden gesteld aan de toegang tot het aantal en/of de soort persoonsgegevens van leerlingen, maar dat valt niet binnen de scope van dit onderzoek.
[15] Artikel 9.2.1 NEN 27002
[16] Artikel 9.2.2 NEN 27002
[17] Artikel 9.2.1 en 9.2.2 NEN 27002
[18] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 12.4.1 NEN 27002
[19] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 12.4.1 NEN 27002

a. Naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens van de leerling;
b. Persoonsgebonden nummer[20];
c. Nationaliteit en geboorteplaats;
d. Gegevens als bedoeld onder a. van de ouders, voogden of verzorgers van de leerling;
e. Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling;
f. Gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het onderwijs;
g. Gegevens betreffende de aard en het verloop van het onderwijs alsmede de behaalde resultaten;
h. Gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen;
i. Gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, onderwijs- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten;
j. Foto´s en videobeelden met of zonder geluid van activiteiten van de onderwijsinstelling;
k. Gegevens van docenten en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van de onderwijsinstelling en het geven van onderwijs;
l. Andere dan de onder a. tot en met k. bedoelde gegevens waarvan de verwerking door de onderwijsinstelling wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van wet-of regelgeving.

2.2.2 Rollen van medewerkers

BOOR heeft in haar brief van 15 juli 2016 aangegeven dat aan de medewerkers van haar onderwijsinstellingen een rol wordt toegekend voor de toegang tot persoonsgegevens van leerlingen in leerlingvolgsysteem X. Leerlingvolgsysteem X kent volgens BOOR de volgende rollen:

- Applicatiebeheerder;
- Administratie;
- Intern begeleider;
- Leerkracht;
- Leerkracht beperkt;
- Accountbeheerder.

2.2.3 Toegang

BOOR heeft in haar brief van 15 juli 2016 aangegeven dat de medewerkers van haar onderwijsinstellingen toegang tot persoonsgegevens van leerlingen in leerlingvolgsysteem X verkrijgen die aan hun rol zijn toegewezen. Tot welke persoonsgegevens van leerlingen de medewerkers toegang hebben, is afhankelijk van de rol die aan de medewerkers is verleend. Schematisch kan dit als volgt worden weergegeven:

[20] Het persoonsgebonden nummer (ook wel onderwijsnummer genoemd) betreft meestal het bsn van de leerling.

			Rollen					
			Applicatiebeheerder	Administratie	Intern begeleider	Leerkracht	Leerkracht beperkt	Accountbeheer
Persoonsgegevens van leerlingen	a.	Contactgegevens leerling	X	X	X	X	X	
	b.	Persoonsgebonden nummer	X	X	X	X	X	
	c.	Nationaliteit en geboorteplaats	X	X	X	X	X	
	d.	Contactgegevens ouders	X	X	X	X	X	
	e.	Gezondheid of welzijn	X	X	X	X	X	
	f.	Godsdienst of levensovertuiging	X	X	X	X	X	
	g.	Aard en verloop onderwijs en behaalde resultaten	X		X	X	X	
	h.	Organisatie onderwijs en verstrekken van leermiddelen	X	X	X	X	X	
	i.	Berekenen, vastleggen en innen van gelden	X	X				
	j.	Foto´s en videobeelden van activiteiten						
	k.	Gegevens van docenten en begeleiders	X	X	X	X	X	X
	l.	Andere gegevens voor toepassing van wet-or regelgeving	X	X				

BOOR heeft aanvankelijk in haar brief van 22 augustus 2016 aangegeven dat de rollen van medewerkers op schoolniveau worden toegekend. Dit betekent dat de toegang van medewerkers van haar onderwijsinstellingen tot de persoonsgegevens van leerlingen in leerlingvolgsysteem X niet is beperkt tot bepaalde (groepen) leerlingen, maar geldt voor alle leerlingen binnen de betreffende onderwijsinstelling.

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft BOOR in haar brief van 30 juni 2017 aangegeven dat zij overleg heeft gevoerd met de uitgever van leerlingvolgsysteem X. Het resultaat hiervan is volgens BOOR dat binnen leerlingvolgsysteem X een functionaliteit tot groepsautorisatie bestaat. Hiermee kan per medewerker worden ingesteld dat men alleen toegang krijgt tot de groep(en) waaraan men expliciet verbonden is. Tevens heeft BOOR aangegeven dat zij de groepsautorisaties heeft toegekend. Bij haar brief van 13 november 2017 heeft BOOR een autorisatielijst van één van onder haar ressorterende onderwijsinstellingen overgelegd.

2.2.4 Procedures toegangsverlening

BOOR heeft aanvankelijk in haar brief van 22 november 2016 aangegeven dat op de toewijzing van toegangsrechten aan de medewerkers van haar onderwijsinstellingen het BOOR directiestatuut[21] van toepassing is. Volgens BOOR is hieruit af te leiden dat de (bovenschools) directeuren gebruikers toegang geven tot leerlingvolgsysteem X in samenhang met de functie die deze gebruikers op de scholen vervullen.

Nadat de AP het rapport van voorlopige bevindingen had vastgesteld en verstuurd, heeft BOOR bij brief van 30 juni 2017 de Procedure autorisatie en logging[22] toegestuurd.

[21] Managementstatuut stichting BOOR-po, 26 mei 2014
[22] Procedure autorisatie en logging LOVS/LAS, versie 1.0, 28 juni 2017, vastgesteld door CVB op 3 juli 2017

2.2.5 Noodzaak toegang

BOOR heeft aanvankelijk in haar brief van 22 augustus 2016 aangegeven dat de toegang in leerlingvolgsysteem X voor alle medewerkers van een onderwijsinstelling tot de persoonsgegevens van alle leerlingen van die onderwijsinstelling noodzakelijk is omdat:

- *Leerkrachten moeten kunnen invallen in andere klassen;*
- *Het wenselijk is om intercollegiaal te kunnen toetsen;*
- *Het wenselijk is om studieresultaten te kunnen vergelijken;*
- *Het wenselijk is om de ontwikkeling van leerlingen te kunnen volgen (longitudinaal onderzoek);*
- *(Indien van toepassing) de schoolmedewerkers met het vervolgonderwijs moeten kunnen overleggen;*
- *(Indien van toepassing) er geschakeld moet kunnen worden met andere instanties die een rol hebben bij de wettelijke taakvervulling om onderwijs te verzorgen.*

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft BOOR in haar brief van 30 juni 2017 aangegeven dat zij groepsautorisaties heeft toegekend.

2.2.6 Logbestanden

BOOR heeft in haar brief van 22 november 2016 aangegeven dat de activiteiten die medewerkers van haar scholen uitvoeren binnen leerlingvolgsysteem X worden gelogd. Per e-mail van 20 januari 2017 heeft BOOR een afschrift van de logbestanden betreffende de periode 4 december 2016 tot en met 2 januari 2017 verstrekt.

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft BOOR in haar brief van 30 juni 2017 aangegeven dat zij in overleg is getreden met de uitgever van leerlingvolgsysteem X, Het resultaat hiervan is volgens BOOR dat leerlingvolgsysteem X uiterlijk per 1 september 2017 loggen conform Richtsnoeren Beveiliging van persoonsgegevens en NEN 27002 mogelijk zal maken. In haar brief van 6 september 2017 heeft BOOR aangegeven dat de activiteiten die de medewerkers van BOOR uitvoeren binnen leerlingvolgsysteem X vanaf de augustus release van leerlingvolgsysteem X worden gelogd conform de Richtsnoeren Beveiliging van persoonsgegevens en NEN 27002. Bij brief van 13 november 2017 heeft BOOR een afschrift van de logbestanden betreffende de periode 30 september tot 31 oktober 2017 verstrekt.

2.2.7 Beoordeling logbestanden

BOOR heeft aanvankelijk in haar brief van 22 november 2016 aangegeven dat de logbestanden op dat moment niet periodiek worden gecontroleerd. Indien gewenst (bij een vermoeden van misbruik) kunnen de logbestanden worden opgevraagd bij de leverancier van leerlingvolgsysteem X.

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft BOOR in haar brief van 30 juni 2017 aangegeven dat zij in overleg is getreden met de uitgever van leerlingvolgsysteem X. Het resultaat hiervan is volgens BOOR dat leerlingvolgsysteem X uiterlijk per 1 september 2017 de functionaliteit loggen beschikbaar zal stellen aan de scholen. BOOR zal per 1 september 2017 de logbestanden periodiek beoordelen met een minimum van eens per twee maanden. Bij deze brief heeft

BOOR haar Procedure autorisatie en logging overgelegd.[23] Een onderdeel van deze rapportage is de Procedure controleren logregels. In haar brief van 6 september 2017 heeft BOOR aangegeven dat de eerste loggings in oktober 2017 worden uitgevoerd, tenzij er aanleiding is om dit eerder uit te voeren. Bij brief van 13 november 2017 heeft BOOR een rapportage van de beoordeling van de logbestanden ten aanzien van één van haar onderwijsinstellingen overgelegd. Bij brief van 11 december 2017 heeft BOOR een toelichting gegeven op de Procedure controleren logregels.

2.3 Beoordeling

2.3.1 Verantwoordelijke

Op grond van artikel 1, sub d, Wbp[24] is de verantwoordelijke degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

BOOR is het bevoegd gezag van 82 scholen in Rotterdam. Zij beslist over de verwerking van persoonsgegevens van leerlingen van de onder haar ressorterende onderwijsinstellingen en het gebruik van leerlingvolgsysteem X daarbij. BOOR is derhalve in deze aan te merken als verantwoordelijke in de zin van de Wbp.

2.3.2 Formele procedure toegangsverlening

De Richtsnoeren Beveiliging van persoonsgegevens en de NEN 27002 vereisen dat er een formele registratie- en afmeldingsprocedure is om toewijzing van de toegangsrechten aan de medewerkers mogelijk te maken[25] en een formele gebruikerstoegangsverleningsprocedure om toegangsrechten voor alle typen gebruikers toe te wijzen of in te trekken.[26] Deze procedures dienen te zijn geïmplementeerd.[27]

BOOR heeft aanvankelijk bij brief van 22 november 2016 het BOOR directiestatuut[28] als formele procedure voor toegangsverlening van de medewerkers van haar onderwijsinstellingen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X overgelegd. Het BOOR directiestatuut bevat evenwel geen procedure omtrent de registratie en afmelding van medewerkers van een onderwijsinstelling en ook niet omtrent het verlenen, wijzigen en intrekken van toegangsrechten tot persoonsgegevens van leerlingen in leerlingvolgsysteem X.

Gelet op het vorenstaande was de AP in het rapport van voorlopige bevindingen van oordeel dat BOOR op dit onderdeel niet voldeed aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens[29] en artikel 9.2.1 en 9.2.2 NEN 27002. BOOR handelde daarmee op dit onderdeel in strijd met artikel 13 Wbp[30].

Nadat de AP het rapport van voorlopige bevindingen had vastgesteld en verstuurd, heeft BOOR bij brief van 30 juni 2017 evenwel de Procedure autorisatie en logging[31] toegestuurd. Hierin is (schematisch)

[23] *Procedure autorisatie en logging, LOVS/LAS*, versie 1.0, 28 juni 2017, vastgesteld door CVB op 3 juli 2017.
[24] Vanaf 25 mei 2018 artikel 4, lid 7, AVG.
[25] Artikel 9.2.1 NEN 27002
[26] Artikel 9.2.2 NEN 27002
[27] Artikel 9.2.1 en 9.2.2 NEN 27002
[28] Managementstatuut stichting BOOR-po, 26 mei 2014
[29] p. 22
[30] Vanaf 25 mei 2018 artikel 32 AVG.
[31] Procedure autorisatie en logging LOVS/LAS, versie 1.0, 28 juni 2017, vastgesteld door CVB op 3 juli 2017

weergegeven het proces van het bepalen van de functie/rol van een medewerker en de groepsautorisatie, alsook het toekennen en intrekken van de autorisatie.

Gelet op het vorenstaande is de AP van oordeel dat BOOR thans op dit onderdeel voldoet aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens[32] en artikel 9.2.1 en 9.2.2 NEN 27002. De AP concludeert aldus dat BOOR thans op dit onderdeel in overeenstemming met artikel 13 Wbp[33] handelt.

2.3.3 Toegangsverlening

De Richtsnoeren beveiliging van persoonsgegevens vereisen dat de medewerkers van de onderwijsinstellingen van BOOR slechts toegang mogen verkrijgen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X die zij voor de uitvoering van hun taken nodig hebben.[34] Dit betekent dat er grenzen dienen te worden gesteld aan de kring van medewerkers die toegang verkrijgen tot persoonsgegevens van een leerling. Wanneer deze grenzen niet of onvoldoende worden gesteld, dan bestaat er het risico dat medewerkers van de onderwijsinstellingen van BOOR onrechtmatig (bijzondere) persoonsgegevens van leerlingen raadplegen, wijzigen, wissen of verstrekken aan derden. Bovendien zijn de gevolgen van een mogelijk beveiligingsincident groter. Wanneer een onbevoegde de inlogcodes van een medewerker weet te achterhalen, verkrijgt hij immers toegang tot een grote set aan (bijzondere) persoonsgegevens.

In het algemeen geldt dat niet alle medewerkers standaard en continu toegang nodig hebben tot persoonsgegevens van (alle) leerlingen voor de uitvoering van hun taken. Zo zal een leerkracht of invalkracht doorgaans onderwijs geven aan een bepaalde groep of bepaalde groepen leerlingen en geen taken uitvoeren ten aanzien van alle leerlingen van een onderwijsinstelling. Ook een intern begeleider zal doorgaans slechts bepaalde leerlingen begeleiden en geen taken uitvoeren ten aanzien van alle leerlingen.

Gelet op het vorenstaande dienen de onderwijsinstellingen van BOOR in ieder geval de volgende stappen te nemen tot het toewijzen van toegangsrechten aan een medewerker:

- bepaal welke rol(len) een medewerker krijgt;
- bepaal ten aanzien van welke (groep(en)) leerlingen de medewerker zijn taken gaat uitvoeren;
- bepaal welke persoonsgegevens van de leerlingen de medeweker nodig heeft om zijn taken goed te kunnen uitvoeren;
- bepaal binnen welke tijdsperiode de medewerker de persoonsgegevens van de leerlingen nodig heeft om zijn taken goed te kunnen uitvoeren.

De medewerkers van de onderwijsinstellingen van BOOR verkregen aanvankelijk alleen toegang tot persoonsgegevens van leerlingen op basis van rollen. Dit werd met technologische middelen afgedwongen. Hierdoor verkregen de medewerkers geen toegang tot andere of meer persoonsgegevens dan aan hun rol was toegewezen. De toegang was evenwel niet beperkt tot bepaalde (groepen) leerlingen en ook niet in tijd, maar gold standaard en continu voor alle leerlingen binnen de betreffende onderwijsinstelling. Ten aanzien van hetgeen BOOR in haar brief van 22 augustus 2016 heeft aangevoerd over de noodzaak van deze toegang tot de persoonsgegevens van alle leerlingen van die onderwijsinstelling, merkt de AP het volgende op:

[32] p. 22
[33] Vanaf 25 mei 2018 artikel 32 AVG.
[34] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 9.2 NEN 27002

Voor bepaalde medewerkers van een onderwijsinstelling kan het voor de uitvoering van hun taken nodig zijn dat zij toegang hebben tot persoonsgegevens van alle leerlingen van een onderwijsinstelling[35], maar dit geldt niet (standaard) voor alle medewerkers. Een leerkracht of een invalkracht bijvoorbeeld zal doorgaans niet (continu) taken uitvoeren met betrekking tot alle leerlingen. Als een leerkracht of invalkracht invalt in een (andere) groep is het veelal op dat moment en voor die periode pas nodig dat de leerkracht of invalkracht toegang krijgt tot persoonsgegevens van de betreffende leerlingen.

Ook kan het tot de taak van leerkrachten behoren dat zij toetsresultaten vergelijken en beoordelen van andere leerlingen dan aan wie zij lesgeven. Maar daarmee is niet onderbouwd, noch is gebleken, de noodzaak dat alle medewerkers standaard en continu toegang moeten hebben tot persoonsgegevens van alle leerlingen. Er is enkel gesteld dat dit wenselijk is. Ook in deze situatie geldt dat de leerkracht pas op dat moment en voor de betreffende periode toegang mag krijgen tot persoonsgegevens van de betreffende leerlingen, voor zover de persoonsgegevens nodig zijn voor het vergelijken en beoordelen van de toetsresultaten.

Ten aanzien van nodige contacten met andere instanties ziet de AP eveneens niet in waarom het nodig is dat de medewerkers van een onderwijsinstelling standaard en continu toegang krijgen tot de persoonsgegevens van alle leerlingen. Ook dit is niet nader door BOOR onderbouwd.

Gelet op het vorenstaande was de AP in het rapport van voorlopige bevindingen van oordeel dat BOOR op dit onderdeel niet voldeed aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens[36]. BOOR handelde daarmee op dit onderdeel in strijd met artikel 13 Wbp[37].

Nadat de AP het rapport van voorlopige bevindingen had vastgesteld en verstuurd, heeft BOOR in haar brief van 30 juni 2017 evenwel aangegeven dat zij groepsautorisaties heeft toegekend. Bij haar brief van 13 november 2017 heeft BOOR een autorisatielijst van één van onder haar ressorterende onderwijsinstellingen overgelegd waaruit blijkt dat zij de groepsautorisaties heeft doorgevoerd. Door het toepassen van groepsautorisaties kan worden bewerkstelligd dat de medewerkers van de onderwijsinstellingen van BOOR slechts toegang verkrijgen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X die zij voor de uitvoering van hun taken nodig hebben.

Gelet op het vorenstaande is de AP van oordeel dat BOOR thans op dit onderdeel voldoet aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens[38]. De AP concludeert aldus dat BOOR thans op dit onderdeel in overeenstemming met artikel 13 Wbp[39] handelt.

2.3.4 Logbestanden

De Richtsnoeren Beveiliging van persoonsgegevens en de NEN 27002 vereisen dat er logbestanden worden gemaakt van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren.[40] Tevens vereist de NEN 27002 dat de logbestanden,

[35] Zoals bijvoorbeeld een administratief medeweker die de administratieve handelingen verricht ten aanzien van alle leerlingen of een applicatiebeheerder die aan alle medewerkers van een onderwijsinstelling de nodige technische ondersteuning biedt bij het gebruik van leerlingvolgsysteem X.
[36] p. 22
[37] Vanaf 25 mei 2018 artikel 32 AVG.
[38] p. 22
[39] Vanaf 25 mei 2018 artikel 32 AVG.
[40] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 12.4.1 NEN 27002

voor zover relevant, een aantal aspecten dienen te bevatten. Eén van deze aspecten betreft de bestanden die zijn geopend en het type toegang dat is verkregen.[41]

BOOR heeft aanvankelijk per e-mail van 20 januari 2017 een afschrift van logbestanden van activiteiten van medewerkers van een onderwijsinstelling binnen leerlingvolgsysteem X betreffende de periode 4 december 2016 tot en met 2 januari 2017 verstrekt. De AP constateerde in het rapport van voorlopige bevindingen dat deze logbestanden evenwel geen informatie bevatten waaruit kan worden afgeleid welke bestanden van een leerling zijn gelezen of aangepast.
Gelet op het vorenstaande was de AP in het rapport van voorlopige bevindingen van oordeel dat BOOR op dit onderdeel niet voldeed aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens[42] en artikel 12.4.1 NEN 27002. BOOR handelde daarmee op dit onderdeel in strijd met artikel 13 Wbp[43].

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft BOOR in haar brief van 30 juni 2017 aangegeven dat zij in overleg is getreden met de uitgever van leerlingvolgsysteem X, Het resultaat hiervan is volgens BOOR dat leerlingvolgsysteem X uiterlijk per 1 september 2017 loggen conform Richtsnoeren Beveiliging van persoonsgegevens en NEN 27002 mogelijk zal maken. In haar brief van 6 september 2017 heeft BOOR aangegeven dat de activiteiten die de medewerkers van BOOR uitvoeren binnen leerlingvolgsysteem X vanaf de augustus release van leerlingvolgsysteem X worden gelogd conform de Richtsnoeren Beveiliging van persoonsgegevens en NEN 27002. Bij brief van 13 november 2017 heeft BOOR een afschrift van de logbestanden van een onderwijsinstelling betreffende de periode 30 september tot 31 oktober 2017 verstrekt. Hieruit blijkt welke bestanden van een leerling zijn gelezen of aangepast.

Gelet op het vorenstaande is de AP van oordeel dat BOOR thans op dit onderdeel voldoet aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens[44] en artikel 12.4.1 NEN 27002. De AP concludeert aldus dat BOOR thans op dit onderdeel in overeenstemming met artikel 13 Wbp[45] handelt.

2.3.5 Beoordeling logbestanden

De Richtsnoeren Beveiliging van persoonsgegevens en de NEN 27002 vereisen dat de logbestanden regelmatig worden beoordeeld.[46] BOOR heeft aanvankelijk in haar brief van 22 november 2016 aangegeven dat de logbestanden op dat moment niet periodiek worden gecontroleerd.

Gelet op het vorenstaande was de AP in het rapport van voorlopige bevindingen van oordeel dat BOOR op dit onderdeel niet voldeed aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens[47] en artikel 12.4.1 NEN 27002. BOOR handelde daarmee op dit onderdeel in strijd met artikel 13 Wbp[48].

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft BOOR in haar brief van 30 juni 2017 aangegeven dat zij per 1 september 2017 de logbestanden periodiek zal beoordelen met een minimum van eens per twee maanden. Bij deze brief heeft BOOR haar Procedure autorisatie en

[41] Artikel 2.4.1, sub j, NEN 27002
[42] p. 22
[43] Vanaf 25 mei 2018 artikel 32 AVG.
[44] p. 22
[45] Vanaf 25 mei 2018 artikel 32 AVG.
[46] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 12.4.1 NEN 27002
[47] p. 22
[48] Vanaf 25 mei 2018 artikel 32 AVG.

logging overgelegd.[49] Een onderdeel van deze rapportage is de Procedure controleren logregels. In haar brief van 6 september 2017 heeft BOOR aangegeven dat de eerste loggings in oktober 2017 worden uitgevoerd, tenzij er aanleiding is om dit eerder uit te voeren. Bij brief van 13 november 2017 heeft BOOR een rapportage van de beoordeling van de logbestanden ten aanzien van één van haar onderwijsinstellingen overgelegd. Uit deze rapportage blijkt dat er geen bijzonderheden zijn geconstateerd. Bij brief van 11 december 2017 heeft BOOR een toelichting gegeven op de Procedure controleren logregels. Daarmee heeft BOOR verduidelijkt waarop zij de logbestanden controleert.

Gelet op het vorenstaande is de AP van oordeel dat BOOR thans op dit onderdeel voldoet aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens[50] en artikel 12.4.1 NEN 27002. De AP concludeert aldus dat BOOR thans op dit onderdeel in overeenstemming met artikel 13 Wbp[51] handelt.

[49] *Procedure autorisatie en logging, LOVS/LAS*, versie 1.0, 28 juni 2017, vastgesteld door CVB op 3 juli 2017.
[50] p. 22
[51] Vanaf 25 mei 2018 artikel 32 AVG.

3. Conclusie

De AP concludeert dat BOOR een formele procedure heeft om de medewerkers van haar onderwijsinstellingen toegang te verlenen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X. De toegangsverlening heeft bovendien slechts betrekking tot persoonsgegevens van leerlingen die de medewerkers voor de uitvoering van hun taken nodig hebben[52]. Verder worden er logbestanden gemaakt van gebeurtenissen binnen leerlingvolgsysteem X die gebruikersactiviteiten van de medewerkers van de onderwijsinstellingen van BOOR, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren. De logbestanden worden regelmatig door BOOR beoordeeld.

BOOR heeft op deze onderdelen voldoende passende maatregelen ten uitvoer gelegd om de persoonsgegevens van leerlingen in leerlingvolgsysteem X te beveiligen tegen onbevoegde kennisneming, wijziging of verstrekking van de gegevens door medewerkers. BOOR handelt daarmee in overeenstemming met artikel 13 Wbp[53].

[52] CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 9.2 NEN 27002
[53] Vanaf 25 mei 2018 artikel 32 AVG.

AUTORITEIT
PERSOONSGEGEVENS

Contactgegevens

Bezoekadres
(alleen volgens afspraak)
Bezuidenhoutseweg 30
2594 AV DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres
Postbus 93374
2509 AJ DEN HAAG

Telefonisch spreekuur
Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer **0900-2001 201**. De publieksvoorlichters zijn bereikbaar op werkdagen van 10.00 tot 12.00 uur en van 14:00 tot 16:00 uur (5 cent per minuut, plus de kosten voor het gebruik van uw mobiele of vaste telefoon).

Persvoorlichting
Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens via telefoonnummer **070-8888 555**.

Zakelijke relaties
Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer **070-8888 500**.