



Onderzoeksrapport

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

## Rapport definitieve bevindingen

# Januari 2018



# Inhoudsopgave

<b>1.</b>	<b>Inleiding</b>	<b>3</b>
1.1	Aanleiding onderzoek	3
1.2	Leerlingvolgsysteem X	3
1.3	Organisatiebeschrijving ASKO	3
1.4	Doel onderzoek	4
1.5	Onderzoeksvragen	4
1.6	Verloop onderzoek	4
1.7	Wettelijk kader	5
1.7.1	Verantwoordelijke	5
1.7.2	Beveiliging	5
<b>2.</b>	<b>Bevindingen</b>	<b>7</b>
2.1	Uitwerking van het wettelijk kader	7
2.2	Feitelijke bevindingen	7
2.2.1	Persoonsgegevens	7
2.2.2	Rollen	8
2.2.3	Toegang	8
2.2.4	Procedures toegangsverlening	9
2.2.5	Noodzaak toegang	10
2.2.6	Logbestanden	11
2.2.7	Beoordeling logbestanden	11
2.3	Beoordeling	11
2.3.1	Verantwoordelijke	11
2.3.2	Formele procedure toegangsverlening	12
2.3.3	Toegangsverlening	12
2.3.4	Logbestanden	15
2.3.5	Beoordeling logbestanden	15
<b>3.</b>	<b>Conclusie</b>	<b>17</b>



# 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<sup>1</sup>, en het feit dat kinderen zijn aan te merken als kwetsbare personen<sup>2</sup>, 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.<sup>3</sup>

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 ASKO

De Amsterdamse Stichting voor Katholiek, Protestants-Christelijk en Interconfessioneel Onderwijs (ASKO) is de grootste organisatie voor primair katholiek/oecumenisch onderwijs in Amsterdam en omstreken. In totaal zijn er 32 scholen met ongeveer 900 medewerkers en ongeveer 9.200 leerlingen.<sup>4</sup> ASKO is één van de grootste besturen die leerlingvolgsysteem X in gebruik heeft.

---

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> Agenda 2016, p.3

([https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/autoriteit\\_persoonsgegevens\\_agenda\\_2016.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/autoriteit_persoonsgegevens_agenda_2016.pdf))

<sup>4</sup> Bron: [www.askoscholen.nl/Paginas/ASKO.aspx](http://www.askoscholen.nl/Paginas/ASKO.aspx)



## 1.4 Doel onderzoek

Het onderzoek beoogt vast te stellen of ASKO passende beveiligingsmaatregelen ten uitvoer heeft geleegd om de persoonsgegevens van leerlingen in leerlingvolgsysteem X te beveiligen tegen onbevoegde kennismaking, 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 ASKO 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 ASKO 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 ASKO 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 ASKO 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 ASKO verzocht om inlichtingen. ASKO heeft bij brief van 24 juni 2016 verzocht om uitstel van reactie. De AP heeft bij brief van 4 juli 2016 uitstel verleend. ASKO heeft bij brief van 14 juli 2016 inlichtingen verstrekt.

De AP heeft bij brief van 26 juli 2016 ASKO verzocht om nadere inlichtingen. ASKO heeft op 29 juli 2016 telefonisch verzocht om uitstel van reactie. De AP heeft telefonisch en per e-mail van 29 juli 2016 uitstel verleend. ASKO heeft per e-mail van 4 september 2016 opnieuw verzocht om uitstel van reactie. De AP heeft per e-mail van 5 september 2016 uitstel verleend. ASKO heeft bij brief van 9 september 2016 inlichtingen verstrekt.

De AP heeft bij brief van 8 november 2016 ASKO verzocht om nadere inlichtingen. ASKO heeft per e-mail van 18 november 2016 verzocht om uitstel van reactie. De AP heeft per e-mail van 21 november 2016



uitstel verleend. ASKO heeft bij brief van 2 december 2016 (tevens per e-mail van 5 december 2016) inlichtingen verstrekt.

De AP heeft bij brief van 3 januari 2017 ASKO verzocht om nadere inlichtingen. ASKO heeft per e-mail van 18 januari 2017 verzocht om uitstel van reactie. De AP heeft per e-mail van 19 januari 2017 uitstel verleend. ASKO heeft per e-mail van 7 februari 2017 inlichtingen verstrekt.

De AP heeft bij brief van 22 mei 2017 het rapport van voorlopige bevindingen betreffende het uitgevoerde onderzoek toegestuurd. De AP heeft ASKO daarbij in de gelegenheid gesteld om schriftelijk haar reactie op dit rapport te geven. ASKO heeft per e-mail van 26 mei 2017 verzocht om uitstel van reactie. De AP heeft per e-mail van 26 mei 2017 uitstel verleend. ASKO heeft telefonisch op 23 juni 2017 opnieuw verzocht om uitstel van reactie. De AP heeft per e-mail van 23 juni 2017 geen uitstel verleend. ASKO heeft bij brief van 29 juni 2017 een schriftelijke reactie gegeven op het rapport van voorlopige bevindingen.

De AP heeft bij brief van 17 juli 2017 ASKO verzocht om inlichtingen. ASKO heeft bij brief van 5 augustus 2017, ontvangen op 6 september 2017, inlichtingen verstrekt.

De AP heeft bij brief van 31 oktober 2017 ASKO verzocht om inlichtingen. ASKO heeft bij brief en per e-mail van 13 november 2017 inlichtingen verstrekt.

## 1.7 Wettelijk kader

### 1.7.1 Verantwoordelijke<sup>5</sup>

Ingevolge artikel 1, sub d, Wbp<sup>6</sup> 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.<sup>7</sup>*

### 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

<sup>5</sup> In de AVG aangeduid als 'verwerkingsverantwoordelijke'.

<sup>6</sup> Vanaf 25 mei 2018 artikel 4, lid 7, AVG.

<sup>7</sup> Kamerstukken II 1997/98, 25 892, nr. 3, p. 55



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 van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.<sup>8</sup>

De AP (destijds het College bescherming persoonsgegevens) heeft in haar Richtsnoeren beveiliging van persoonsgegevens<sup>9</sup> 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<sup>10</sup> (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.

---

<sup>8</sup> 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.

<sup>9</sup> CBP Richtsnoeren *Beveiliging van persoonsgegevens*, februari 2013 (<https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-richtsnoeren-beveiliging-van-persoonsgegevens>)

<sup>10</sup> 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 wettelijk kader

Ingevolge artikel 13 Wbp dient ASKO 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.<sup>11</sup>

ASKO dient derhalve (onder andere) beveiligingsmaatregelen te treffen om toegang tot persoonsgegevens van leerlingen in leerlingvolgsysteem X voor bevoegde medewerkers van haar onderwijsinstellingen te bewerkstelligen en onbevoegde toegang tot deze persoonsgegevens te voorkomen.<sup>12</sup> De volgende aspecten van de Richtsnoeren Beveiliging van persoonsgegevens en de NEN 27002 zijn betrokken bij de beoordeling of ASKO passende beveiligingsmaatregelen 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 ASKO toegang te geven tot persoonsgegevens van leerlingen in leerlingvolgsysteem X die zij voor de uitvoering van hun taken nodig hebben<sup>13 14</sup>:
  - Er dient een formele registratie- en afmeldingsprocedure te zijn om toewijzing van de toegangsrechten aan de medewerkers mogelijk te maken<sup>15</sup> alsmede een formele gebruikerstoegangsverleningsprocedure om toegangsrechten voor alle typen gebruikers toe te wijzen of in te trekken<sup>16</sup>.
  - Deze procedures dienen te zijn geïmplementeerd.<sup>17</sup>
- Er dienen logbestanden te worden gemaakt van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren.<sup>18</sup>
- De logbestanden dienen regelmatig te worden beoordeeld.<sup>19</sup>

### 2.2 Feitelijke bevindingen

#### 2.2.1 Persoonsgegevens

ASKO heeft in haar brief van 14 juli 2016 aangegeven dat de volgende persoonsgegevens van leerlingen van haar onderwijsinstellingen in leerlingvolgsysteem X worden verwerkt:

---

<sup>11</sup> *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.

<sup>12</sup> CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 9.2 NEN 27002

<sup>13</sup> CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 9.2 NEN 27002

<sup>14</sup> 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.

<sup>15</sup> Artikel 9.2.1 NEN 27002

<sup>16</sup> Artikel 9.2.2 NEN 27002

<sup>17</sup> Artikel 9.2.1 en 9.2.2 NEN 27002

<sup>18</sup> CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 12.4.1 NEN 27002

<sup>19</sup> 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<sup>20</sup>;
- 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 leskosten 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

ASKO heeft in haar brief van 14 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 ASKO de volgende rollen:

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

### 2.2.3 Toegang

ASKO heeft in haar brief van 14 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:

---

<sup>20</sup> 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				

ASKO heeft aanvankelijk in haar brief van 9 september 2016 aangegeven 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 ASKO in haar brief van 29 juni 2017 aangegeven dat zij in overleg is getreden met de uitgever van leerlingvolgsysteem X. Het resultaat hiervan is volgens ASKO dat binnen leerlingvolgsysteem X een nieuwe optie groepsautorisatie bestaat. Hiermee kan per medewerker worden ingesteld dat men alleen toegang krijgt tot de groep(en) waaraan men expliciet verbonden is. Tevens heeft ASKO aangegeven dat zij de groepsautorisatie uiterlijk per 1 augustus 2017 implementeert. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat zij per 1 augustus 2017 de groepsautorisatie heeft toegepast op de accounts van de medewerkers. Bij haar brief van 13 november 2017 heeft ASKO een autorisatielijst van één van onder haar ressorterende onderwijsinstellingen overgelegd.

#### 2.2.4 Procedures toegangsverlening

ASKO heeft aanvankelijk in haar brief van 2 december 2016 aangegeven dat bij indiensttreding accounts met de juiste autorisatie voor diverse applicaties worden aangemaakt. Bij vertrek van een medewerker worden de accounts meteen weer opgeheven dan wel gedeactiveerd. De procedure is onderdeel van het privacyprotocol. Dit protocol bevat hierover het volgende:

*Eén iemand op school moet verantwoordelijk zijn voor het op de agenda houden van het thema privacy van gegevens personeel & leerlingen. Deze persoon moet ook mutaties in het personeelsbestand van de school*



*ogenblikkelijk toepassen op de toegang tot het schoolnetwerk en tot applicaties als leerlingvolgsysteem X. Met name de toegang van personeelsleden die vertrekken moeten terstond geblokkeerd worden.*

Nadat de AP het rapport van voorlopige bevindingen had vastgesteld en verstuurd, heeft ASKO bij brief van 29 juni 2017 de procedure Autorisatie leerlingvolgsysteem X toegestuurd.

#### 2.2.5 Noodzaak toegang

ASKO heeft aanvankelijk in haar brief van 9 september 2016 de noodzaak van de toegang in leerlingvolgsysteem X tot de persoonsgegevens van alle leerlingen van een onderwijsinstelling als volgt gemotiveerd:

*Leerlingvolgsysteem X biedt niet de mogelijkheid om rollen alleen maar toegang te geven tot de persoonsgegevens van specifieke groepen leerlingen. (...) Daarnaast is het de vraag of zo'n beperking vanuit praktisch oogpunt wenselijk is. PO scholen zijn over het algemeen niet al te grote organisaties, waarbij veel verschillende medewerkers te maken hebben met individuele leerlingen.*

ASKO noemt in haar brief van 9 september 2016 de volgende voorbeelden:

*In geval van nood heeft elke personeelslid op school directe toegang nodig tot persoonsgegevens van een leerling, bijvoorbeeld naam, telefoonnummer, noodnummers, gegevens huisarts, medische bijzonderheden.*

*Op elke school zijn personen met de rol leerkracht die te maken hebben met alle leerlingen. Denk aan vaste invalleerkrachten, de leerkracht bewegingsonderwijs, een muziekdocent, een vakleerkracht beeldende vorming. Daarnaast komt het regelmatig voor dat de vaste leerkracht van een specifieke groep lesgeeft in een andere groep.*

*Met betrekking tot de rollen administratie, intern begeleider, applicatiebeheerder en accountbeheer: bij de gemiddelde school slechts 1 persoon deze rol vervullen, waardoor men automatisch toegang heeft tot persoonsgegevens van alle leerlingen op grond van de rechten die bij de rol horen.*

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft ASKO in haar brief van 29 juni 2017 aangegeven dat er een nieuwe optie groepsautorisatie bestaat. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat zij per 1 augustus 2017 de groepsautorisatie heeft toegepast op de accounts van de medewerkers

Tevens heeft ASKO in haar brief van 29 juni 2017 aangegeven dat zij in overleg is getreden met de uitgever van leerlingvolgsysteem X. Het resultaat hiervan is volgens ASKO dat leerlingvolgsysteem X uiterlijk per 1 september 2017 een noodknop zal hebben ontwikkeld. Daarmee wordt het volgens ASKO voor elke medewerker binnen de school mogelijk om tijdelijk (voor maximaal één dag) toegang te krijgen tot de persoonsgegevens van een leerling waartoe men op grond van de groepsautorisatie normaliter geen toegang toe heeft. Bij het aanvragen van de toegang volgt een melding dat men niet bevoegd is om toegang te krijgen tot de persoonsgegevens van deze specifieke leerling. Vervolgens dient men aan te geven waarom toegang tot die gegevens toch noodzakelijk is. Deze actie wordt gelogd door het systeem. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat de noodknop is gebouwd en in de leerlingvolgsysteem X release van 6 september 2017 voor de eindgebruikers ter beschikking zal worden gesteld.



## 2.2.6 Logbestanden

ASKO heeft in haar brief van 2 december 2016 aangegeven dat de activiteiten die medewerkers van haar scholen uitvoeren binnen leerlingvolgsysteem X worden gelogd. Per e-mail van 7 februari 2017 heeft ASKO 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 ASKO in haar brief van 29 juni 2017 aangegeven dat zij in overleg is getreden met de uitgever van leerlingvolgsysteem X. Het resultaat hiervan is volgens ASKO dat leerlingvolgsysteem X per 1 september 2017 loggen conform de Richtsnoeren Beveiliging van persoonsgegevens en de NEN 27002 mogelijk zal maken. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat de activiteiten die de medewerkers van ASKO uitvoeren binnen leerlingvolgsysteem X inmiddels worden gelogd conform de Richtsnoeren Beveiliging persoonsgegevens en de NEN 27002. Per e-mail van 13 november 2017 heeft ASKO een afschrift van de logbestanden betreffende de periode 30 september tot 31 oktober 2017 verstrekt.

## 2.2.7 Beoordeling logbestanden

ASKO heeft aanvankelijk in haar brief van 2 december 2016 aangegeven dat zij niet zelf beschikt over logbestanden. Bij ernstige vermoedens van misbruik kan ASKO zich wenden tot de uitgever van leerlingvolgsysteem X, waarop logbestanden kunnen worden onderzocht.

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft ASKO in haar brief van 29 juni 2017 aangegeven dat zij in overleg is getreden met de uitgever van leerlingvolgsysteem X. Het resultaat hiervan is volgens ASKO dat leerlingvolgsysteem X uiterlijk per 1 september 2017 de functionaliteit loggen beschikbaar zal stellen aan de scholen. Tevens heeft ASKO aangegeven dat zij de logbestanden per 1 september 2017 periodiek zal beoordelen met een minimum van eens per twee maanden. Bij deze brief heeft ASKO haar procedure beoordelen logbestanden leerlingvolgsysteem X overgelegd. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat de logbestanden beschikbaar zijn en voor 1 november 2017 de eerste beoordeling zal plaatsvinden. Bij brief van 13 november 2017 heeft ASKO een rapportage van de beoordeling van de logbestanden leerlingvolgsysteem X ten aanzien van één van haar onderwijsinstellingen overgelegd.

## 2.3 Beoordeling

### 2.3.1 Verantwoordelijke

Op grond van artikel 1, sub d, Wbp<sup>21</sup> is de verantwoordelijke degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

ASKO is het bevoegd gezag van 32 scholen in Amsterdam en omstreken. Zij beslist over de verwerking van persoonsgegevens van leerlingen van de onder haar ressorterende onderwijsinstellingen en het gebruik van leerlingvolgsysteem X daarbij. ASKO is derhalve in deze aan te merken als verantwoordelijke in de zin van de Wbp.

---

<sup>21</sup> Vanaf 25 mei 2018 artikel 4, lid 7, AVG



### 2.3.2 Formele procedure toegangverlening

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<sup>22</sup> en een formele gebruikerstoegangsverleningsprocedure om toegangsrechten voor alle typen gebruikers toe te wijzen of in te trekken.<sup>23</sup> Deze procedures dienen te zijn geïmplementeerd.<sup>24</sup>

ASKO heeft aanvankelijk in haar brief van 2 december 2016 verwezen naar haar privacyprotocol als formele procedure voor toegangverlening van de medewerkers van haar onderwijsinstellingen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X. Hierin staat volgens ASKO dat:

*één iemand op school verantwoordelijke [moet] zijn voor het op de agenda houden van het thema privacy van gegevens van personeel en leerlingen. Deze persoon moet ook mutaties in het personeelsbestand van de school ogenblikkelijk toepassen op de toegang tot het schoolnetwerk en tot applicaties als leerlingvolgsysteem X. Met name de toegang van personeelsleden die vertrekken moeten terstond worden geblokkeerd.*

De enkele regel dat iemand verantwoordelijk dient te zijn voor toegangverlening en –intrekking, betekent evenwel niet dat daarmee ook een formele procedure is vastgesteld omtrent de registratie en afmelding van medewerkers van een onderwijsinstelling en 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 ASKO op dit onderdeel niet voldeed aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens<sup>25</sup> en artikel 9.2.1 en 9.2.2 NEN 27002. ASKO handelde daarmee op dit onderdeel in strijd met artikel 13 Wbp<sup>26</sup>.

Nadat de AP het rapport van voorlopige bevindingen had vastgesteld en verstuurd, heeft ASKO bij haar brief van 29 juni 2017 evenwel de procedure Autorisatie leerlingvolgsysteem X toegestuurd. Hierin is weergegeven het proces van het aanvragen en sluiten van een account leerlingvolgsysteem X, alsook het doorvoeren van mutaties binnen en het deactiveren van het account leerlingvolgsysteem X.

Gelet op het vorenstaande is de AP van oordeel dat ASKO thans op dit onderdeel voldoet aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens<sup>27</sup> en artikel 9.2.1 en 9.2.2 NEN 27002. De AP concludeert aldus dat ASKO thans op dit onderdeel in overeenstemming met artikel 13 Wbp<sup>28</sup> handelt.

### 2.3.3 Toegangsverlening

De Richtsnoeren beveiliging van persoonsgegevens vereisen dat de medewerkers van de onderwijsinstellingen van ASKO slechts toegang mogen verkrijgen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X die zij voor de uitvoering van hun taken nodig hebben.<sup>29</sup> Dit betekent dat er grenzen dienen te worden gesteld aan de kring van medewerkers die toegang verkrijgen tot persoonsgegevens van

---

<sup>22</sup> Artikel 9.2.1 NEN 27002

<sup>23</sup> Artikel 9.2.2 NEN 27002

<sup>24</sup> Artikel 9.2.1 en 9.2.2 NEN 27002

<sup>25</sup> p. 22

<sup>26</sup> Vanaf 25 mei 2018 artikel 32 AVG.

<sup>27</sup> p. 22

<sup>28</sup> Vanaf 25 mei 2018 artikel 32 AVG.

<sup>29</sup> CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 9.2 NEN 27002



een leerling. Wanneer deze grenzen niet of onvoldoende worden gesteld, dan bestaat er het risico dat medewerkers van de onderwijsinstellingen van ASKO 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 invakkracht 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 ASKO 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 medewerker 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 ASKO 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 ASKO in haar brief van 9 september 2016 heeft aangevoerd over de noodzaak van deze toegang tot de persoonsgegevens van alle leerlingen van die onderwijsinstelling, merkt de AP het volgende op:

ASKO heeft aangegeven dat leerlingvolgsysteem X niet de mogelijkheid biedt om rollen alleen maar toegang te geven tot de persoonsgegevens van specifieke groepen leerlingen. De 'huidige stand van de techniek' is evenwel maatgevend voor hetgeen als passend beveiligingsmaatregelen in de zin van artikel 13 Wbp wordt beschouwd. Gelet op de thans beschikbare mogelijkheden om in technische zin te faciliteren dat medewerkers van onderwijsinstellingen van ASKO alleen toegang krijgen tot persoonsgegevens van leerlingen die zij nodig hebben voor de uitvoering van hun taken, voldoet de invulling van toegangsverlening door ASKO niet aan het bepaalde van artikel 13 Wbp.

ASKO heeft aangegeven dat van onderwijsinstellingen wordt verwacht dat zij adequaat optreden in geval van noodsituaties bij leerlingen. Tegelijkertijd is ASKO evenwel ook verantwoordelijk voor de bescherming van de persoonsgegevens van de leerlingen van haar onderwijsinstellingen. ASKO heeft niet nader onderbouwd waarom alle medewerkers van een onderwijsinstelling wegens mogelijke noodsituaties directe toegang nodig hebben tot de persoonsgegevens van alle leerlingen. Niet is onderbouwd of afgewogen waarom niet kan worden volstaan met voorzieningen als een



noodknopprocedure<sup>30</sup> en/of uitzonderingen ten aanzien van specifieke leerlingen. Deze uitzonderingen dienen goed onderbouwd en proportioneel te zijn.

Voorts kan het voor bepaalde medewerkers van een onderwijsinstelling voor de uitvoering van hun taken nodig zijn dat zij toegang hebben tot persoonsgegevens van alle leerlingen van een onderwijsinstelling<sup>31</sup>, 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.

Gelet op het vorenstaande was de AP in het rapport van voorlopige bevindingen van oordeel dat ASKO op dit onderdeel niet voldeed aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens<sup>32</sup>. ASKO handelde daarmee op dit onderdeel in strijd met artikel 13 Wbp<sup>33</sup>.

Nadat de AP het rapport van voorlopige bevindingen had vastgesteld en verstuurd, heeft ASKO in haar brief van 29 juni 2017 evenwel aangegeven dat er een nieuwe optie groepsautorisatie bestaat. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat zij per 1 augustus 2017 de groepsautorisatie heeft toegepast op de accounts van de medewerkers. Bij haar brief van 13 november 2017 heeft ASKO 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 ASKO slechts toegang verkrijgen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X die zij voor de uitvoering van hun taken nodig hebben.

Tevens heeft ASKO in haar brief van 29 juni 2017 aangegeven dat er een noodknop is ontwikkeld. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat de noodknop is gebouwd en in de leerlingvolgsysteem X release van 6 september 2017 voor de eindgebruikers ter beschikking zal worden gesteld. Daarmee wordt het voor elke medewerker binnen de school mogelijk om tijdelijk toegang te krijgen tot de persoonsgegevens van een leerling waartoe men op grond van de groepsautorisatie normaliter geen toegang toe heeft. Ook hierdoor kan worden bewerkstelligd dat de medewerkers van de onderwijsinstellingen van ASKO slechts toegang verkrijgen tot persoonsgegevens van leerlingen in leerlingvolgsysteem X die zij slechts op dat moment voor de uitvoering van hun taken nodig hebben.

Gelet op het vorenstaande is de AP van oordeel dat ASKO thans op dit onderdeel voldoet aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens<sup>34</sup>. De AP concludeert aldus dat ASKO thans op dit onderdeel in overeenstemming met artikel 13 Wbp<sup>35</sup> handelt.

---

<sup>30</sup> Met een noodknopprocedure kunnen medewerkers van onderwijsinstellingen toegang krijgen tot meer persoonsgegevens dan aan hun rol is toegekend. Zo'n procedure kan bijvoorbeeld bestaan uit een extra pop-up op het scherm, waardoor de medewerkers erop worden gewezen dat zij niet bevoegd zijn om toegang te krijgen tot deze specifieke persoonsgegevens. De medewerkers kunnen dan worden gevraagd om een reden aan te geven waarom toegang tot die gegevens toch noodzakelijk is. Met behulp van deze procedure kunnen medewerkers dan alsnog ruimer toegang verkrijgen tot persoonsgegevens van leerlingen.

<sup>31</sup> Zoals bijvoorbeeld een administratief medewerker 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.

<sup>32</sup> p. 22

<sup>33</sup> Vanaf 25 mei 2018 artikel 32 AVG.

<sup>34</sup> p. 22

<sup>35</sup> Vanaf 25 mei 2018 artikel 32 AVG.



#### 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.<sup>36</sup> Tevens vereist de NEN 27002 dat de logbestanden, 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.<sup>37</sup>

ASKO heeft aanvankelijk per e-mail van 7 februari 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 ASKO op dit onderdeel niet voldeed aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens<sup>38</sup> en artikel 12.4.1 NEN 27002. ASKO handelde daarmee op dit onderdeel in strijd met artikel 13 Wbp<sup>39</sup>.

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft ASKO in haar brief van 29 juni 2017 aangegeven dat zij in overleg is getreden met de uitgever van leerlingvolgsysteem X. Het resultaat hiervan is volgens ASKO dat leerlingvolgsysteem X uiterlijk per 1 september 2017 loggen conform de Richtsnoeren Beveiliging van persoonsgegevens en de NEN 27002 mogelijk zal maken. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat de activiteiten die de medewerkers van ASKO uitvoeren binnen leerlingvolgsysteem X inmiddels worden gelogd conform de Richtsnoeren Beveiliging persoonsgegevens en de NEN 27002. Per e-mail van 13 november 2017 heeft ASKO 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 ASKO thans op dit onderdeel voldoet aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens<sup>40</sup> en artikel 12.4.1 NEN 27002. De AP concludeert aldus dat ASKO thans op dit onderdeel in overeenstemming met artikel 13 Wbp<sup>41</sup> handelt.

#### 2.3.5 Beoordeling logbestanden

De Richtsnoeren Beveiliging van persoonsgegevens en de NEN 27002 vereisen dat de logbestanden regelmatig worden beoordeeld.<sup>42</sup> ASKO heeft aanvankelijk in haar brief van 2 december 2016 aangegeven zij niet zelf beschikt over logbestanden. Pas bij ernstige vermoedens van misbruik kan ASKO zich wenden tot de uitgever van leerlingvolgsysteem X waarop logbestanden kunnen worden onderzocht. ASKO controleert de logbestanden dus niet regelmatig.

---

<sup>36</sup> CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 12.4.1 NEN 27002

<sup>37</sup> Artikel 2.4.1, sub j, NEN 27002

<sup>38</sup> p. 22

<sup>39</sup> Vanaf 25 mei 2018 artikel 32 AVG.

<sup>40</sup> p. 22

<sup>41</sup> Vanaf 25 mei 2018 artikel 32 AVG.

<sup>42</sup> CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 12.4.1 NEN 27002





Gelet op het vorenstaande was de AP in het rapport van voorlopige bevindingen van oordeel dat ASKO op dit onderdeel niet voldeed aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens<sup>43</sup> en artikel 12.4.1 NEN 27002. ASKO handelde daarmee op dit onderdeel in strijd met artikel 13 Wbp<sup>44</sup>.

Nadat de AP het rapport van voorlopige bevindingen had opgesteld en verstuurd, heeft ASKO in haar brief van 29 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 ASKO haar procedure beoordelen logbestanden leerlingvolgsysteem X overgelegd. In haar brief van 5 augustus 2017 heeft ASKO aangegeven dat de logbestanden beschikbaar zijn en voor 1 november 2017 de eerste beoordeling zal plaatsvinden. Bij brief van 13 november 2017 heeft ASKO een rapportage van de beoordeling van de logbestanden leerlingvolgsysteem X ten aanzien van één van haar onderwijsinstellingen overgelegd. Uit deze rapportage blijkt dat er geen bijzonderheden zijn geconstateerd.

Gelet op het vorenstaande is de AP van oordeel dat ASKO thans op dit onderdeel voldoet aan de vereisten van de Richtsnoeren Beveiliging van persoonsgegevens<sup>45</sup> en artikel 12.4.1 NEN 27002. De AP concludeert aldus dat ASKO thans op dit onderdeel in overeenstemming met artikel 13 Wbp<sup>46</sup> handelt.

---

<sup>43</sup> p.22

<sup>44</sup> Vanaf 25 mei 2018 artikel 32 AVG.

<sup>45</sup> p. 22

<sup>46</sup> Vanaf 25 mei 2018 artikel 32 AVG.





### 3. Conclusie

De AP concludeert dat ASKO 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<sup>47</sup>. Verder worden er logbestanden gemaakt van gebeurtenissen binnen leerlingvolgsysteem X die gebruikersactiviteiten van de medewerkers van de onderwijsinstellingen van ASKO, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren. De logbestanden worden regelmatig door ASKO beoordeeld.

ASKO 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. ASKO handelt daarmee in overeenstemming met artikel 13 Wbp<sup>48</sup>.

---

<sup>47</sup> CBP Richtsnoeren *Beveiliging van persoonsgegevens*, p. 22 en artikel 9.2 NEN 27002

<sup>48</sup> Vanaf 25 mei 2018 artikel 32 AVG.



## 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](http://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 redacteurs 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.