JBP 2014/99
College bescherming persoonsgegevens
19 september 2014, z2013-00795.
(mr. Kohnstamm
mr. Tomesen)

Onderzoek naar de verwerking van persoonsgegevens door Snappet.

Gebruik persoonsgegevens in onderwijs, Apps

[Wbp - 1 aanhef en onder a, d en e ; Wbp - 8 ; Wbp - 9 ; Wbp - 13 ; Wbp - 14]

» Samenvatting

Snappet verhuurt tablets aan basisscholen waarop onderwijssoftware/-apps zijn geïnstalleerd. Op de Snappet-tablets kunnen kinderen lees- en oefenstof doen voor vakken als taal, spelling, rekenen en lezen. Snappet verwerkt gevoelige persoonsgegevens, nu het gaat om zeer gedetailleerde gegevens over de individuele onderwijsvorderingen van zeven tot negenjarige kinderen. Ten aanzien van zes van de negen doeleinden waarvoor Snappet persoonsgegevens verwerkt stelt het CBP vast dat Snappet niet als bewerker kan optreden. Snappet verwerkt in deze doeleinden enkel gegevens voor zichzelf (en niet voor andere personen of instellingen) of heeft feitelijk teveel zeggenschap over deze doeleinden van de gegevensverwerking om als bewerker te worden aangemerkt. Daarbij worden scholen onjuist geïnformeerd door Snappet dat de overzichten van resultaten per opgave geen persoonsgegevens zouden bevatten, terwijl het om gepseudonimiseerde persoonsgegevens gaat. Door het ontbreken van informatie over essentiële elementen van de gegevensverwerkingen kunnen de scholen doel en middelen van de gegevensverwerking niet bepalen, en dus de zeggenschap niet uitoefenen die vereist is c.q. zou zijn om hun rol als verantwoordelijken te kunnen vervullen.

Voor zes van de verwerkingen waarvoor Snappet de verantwoordelijke is komen in dit geval twee grondslagen in aanmerking: ondubbelzinnige toestemming (artikel 8, aanhef en onder a, van de Wbp) en noodzaak voor gerechtvaardigd belang (artikel 8, aanhef en onder f, van de Wbp). Snappet verkrijgt geen ondubbelzinnige toestemming van de wettelijk vertegenwoordiger(s) van de kinderen voor deze gegevensverwerkingen. Bovendien kan Snappet geen beroep kan doen op een andere grondslag in artikel 8 van de Wbp omdat niet is voldaan aan het proportionaliteitsvereiste en ontbreken waarborgen, zoals de vereiste transparantie over de gegevensverwerkingen. Snappet heeft als verantwoordelijke daarom geen grondslag voor deze gegevensverwerkingen en handelt hierdoor in strijd met artikel 8 van de Wbp.

Daarnaast geldt dat er geen duidelijke verwantschap is tussen de doelen waarvoor de persoonsgegevens worden verzameld en de verdere verwerking ervan. Door de gevoelige aard van de gegevens, de wijze van verzamelen, de gevolgen van de verdere verwerking op de persoonlijke levenssfeer van de kinderen alsmede door het ontbreken van de nodige waarborgen en voorzieningen is de verdere verwerking ervan door Snappet onverenigbaar met de doeleinden waarvoor Snappet de gegevens verkrijgt. Hierdoor handelt Snappet in strijd met artikel 9 van de Wbp.

Ten slotte handelt Snappet in strijd met artikel 13 van de Wbp door het ontbreken van versleuteling, waardoor onbevoegde derde partijen toegang konden krijgen tot de prestaties en vorderingen van de kinderen.

» Uitspraak

De volledige versie van dit rapport is te lezen op www.cbpweb.nl

» Noot

1. Inleiding

Nieuwe technologieën voor onderwijsmateriaal brengen interessante privacy vragen mee. In het oordeel van het CBP dat in deze noot wordt besproken (het "Rapport"), komt het CBP tot de conclusie dat het verwerken van persoonsgegevens van leerlingen door Snappet om meerdere redenen niet door de beugel kan. Die uitkomst is gezien de wijze waarop Snappet haar dienst had ingericht niet verrassend en ook niet onterecht. Dat neemt niet weg dat het CBP in haar oordeel op bepaalde punten wel wat kort door de bocht gaat. In deze noot belicht ik een specifiek onderdeel uit het Rapport, te weten de kwalificatie van de soort verwerkte persoonsgegevens.

2. Pseudoniemen

Volgens het Rapport worden door Snappet in het kader van de onderwijsapps de volgende gegevens van leerlingen verwerkt:

• Voornaam

• Achternaam

• Gebruikersnaam

• UserID

• Wachtwoord (ge-encrypt)

• [VERTROUWELIJK]

• Device ID van de tablet en IP-adres (van de school)

• Leerprestaties: vak/antwoorden op gemaakte opgaven, tijdstip van aanvang en afronding, aantal pogingen en vrije antwoorden

• Tijdstip en duur gebruik van apps

• Scores en vaardigheidsniveaus

• Klas/Groep

• School

Dat dit allemaal persoonsgegevens zijn wanneer deze aan de direct herleidbare gegevens zoals voor- en achternaam en school van leerlingen worden gekoppeld, behoeft geen uitleg. In dat geval is immers duidelijk welke leerling de software op een tablet gebruikt heeft en welke informatie daarbij hoort.

Eén van de doeleinden waarvoor Snappet gegevens over het gebruik van de onderwijsapps door leerlingen gebruikt, is het maken van overzichten van alle behaalde resultaten per opgave door kinderen in een bepaald leerjaar. Op basis hiervan deelt Snappet leerlingen in in bepaalde vaardigheidsniveaus, door de gegevens te vergelijken met de prestaties van andere kinderen in de klas en met alle andere kinderen die de tablets gebruiken.

Deze overzichten worden niet gemaakt op basis van voor-en achternaam of gebruikersnaam, maar op basis van een *gepseudonimiseerde identifier* per kind. De werkwijze die Snappet hanteert om tot een tabel met algemene groepsprestaties per opgave te komen, is gedeeltelijk als vertrouwelijk aangemerkt in het Rapport. Essentieel is echter dat een nieuw, uniek nummer per kind wordt gegenereerd op basis waarvan de tabel tot stand wordt gebracht. Omdat dit nieuwe, unieke nummer met de informatie in de tabel apart wordt opgeslagen van de overige informatie die wel aan direct herleidbare gegevens is gekoppeld (logisch gescheiden), is volgens Snappet voor deze verwerking geen sprake van persoonsgegevens.

Van anonieme gegevens is alleen sprake indien de informatie betrekking heeft op een natuurlijk persoon die niet kan worden geïdentificeerd, noch door de voor de verwerking verantwoordelijke, noch door een ander persoon, rekening houdende met alle middelen waarvan mag worden aangenomen dat zij redelijkerwijze door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn voor de identificatie van de betrokkene (Artikel 29-werkgroep Advies 4/2007 over het begrip persoonsgegeven, p. 19). Dat het met de mogelijkheden van de huidige techniek vrijwel onmogelijk is om persoonsgegevens te anonimiseren terwijl deze nog bruikbaar blijven voor analyse, blijkt wel uit de opinie van Werkgroep 29 over technieken voor anonimisering (Artikel 29-werkgroep Advies 5/2014 over anonimiseringstechnieken).

Ook in het geval van de overzichten op basis van gepseudonimiseerde identifiers is geen sprake van anonieme gegevens. Er worden individuele leerprestaties verwerkt om de groepsprestaties te berekenen en om de individuele prestaties daarmee te vergelijken. Die individuele prestaties zijn volgens het CBP herleidbaar tot de betrokken leerling, omdat de individuele leerprestaties uniek zijn. Met andere woorden, geen twee kinderen zullen precies dezelfde resultaten behalen. Naast de tabel met gegevens op basis van het unieke nummer, beschikt Snappet ook over alle individuele data, per opgave, per kind en per school. Deze oorspronkelijke gegevens in de database waarin de namen en andere gegevens van kinderen zijn opgenomen, kunnen gemakkelijk gekoppeld worden aan alle oorspronkelijke resultaten gekoppeld aan de unieke ID per kind.

Van onomkeerbare anonimisering is dus geen sprake, enkel van pseudonimisering. Gepseudonimiseerde gegevens zijn gewoon persoonsgegevens en vallen binnen de reikwijdte van de Wbp. Dat oordeel is in lijn met overweging 23 van het meest recente voorstel voor de Europese Dataprotectie Verordening (Europese Dataprotectie Verordening, notitie Raad van Europa van 9 maart 2015, 6834/15). In de samenvatting geeft het CBP aan dat sprake is van gevoelige gegevens, omdat het gaat om zeer gedetailleerde gegevens over de individuele onderwijsvorderingen van zeven- tot negenjarige kinderen (Onderzoek naar de verwerking van persoonsgegevens door Snappet, CBP rapport definitieve bevindingen van 14 juli 2014, p. 2);

Pseudonimisering heeft echter wel degelijk voordelen boven het gebruik van direct herleidbare persoonsgegevens, zo wordt ook in de voorgestelde overweging 23a benadrukt. Pseudonimisering kan de risico's voor het verwerken van persoonsgegevens verkleinen en de verantwoordelijke op die manier helpen om aan zijn verplichtingen te voldoen. Het verlies van pseudoniemen is immers veel minder risicovol dan het verlies van niet-gepseudonimiseerde gegevens.

Voor de activiteiten van Snappet uitspraak is bovendien de volgende voorgestelde overweging 23c interessant:

Ik ben het met het CBP eens dat de overzichten op basis van gepseudonimiseerde identifiers per kind geen anonieme gegevens zijn en dus binnen het bereik van de Wbp vallen. Naar mijn mening had het CBP echter wel meer aandacht kunnen geven aan het feit dat een deel van de gegevens gepseudonimiseerd is, bijvoorbeeld het deel van het Rapport dat betrekking heeft op de beveiliging of bij de belangenafweging in het kader van artikel 8 sub f. Het gebruik van pseudoniemen heeft vanwege de verminderde risico's voor betrokkenen de voorkeur boven het gebruik van direct identificerende gegevens en het zou mooi zijn als dat ook door het CBP wat meer benadrukt wordt.

3. Gevoelige persoonsgegevens

Aan de andere kant worden namelijk wel de leerresultaten die door Snappet worden verwerkt, door het CBP aangemerkt als *gevoelige* persoonsgegevens. Maar wat zijn eigenlijk "gevoelige gegevens"?

Het CBP geeft in het Rapport verschillende redenen voor deze kwalificatie van de door Snappet verwerkte gegevens.

Daarna merkt het CBP op dat het gaat om gevoelige gegevens *"waaraan allerlei conclusies kunnen worden verbonden met gevolgen in het (latere) maatschappelijk leven"* (Onderzoek naar de verwerking van persoonsgegevens door Snappet, CBP rapport definitieve bevindingen van 14 juli 2014, p. 5);

Op weer een ander moment geeft het CBP aan dat de persoonsgegevens van leerlingen door Snappet worden gecombineerd met de persoonsgegevens met gegevens over gemaakte opdrachten en technische gegevens over het gebruik van de app. Dat zijn volgens het CBP naar hun aard gegevens over *gedragingen* van een natuurlijke persoon (informatie over zijn of haar schoolprestaties). Door de *context* waarin de gegevens worden gebruikt zijn het volgens het CBP gevoelige gegevens (Onderzoek naar de verwerking van persoonsgegevens door Snappet, CBP rapport definitieve bevindingen van 14 juli 2014, p. 46);

Ten slotte zou het gaan om gezondheidsgegevens: Als Snappet uit de leerprestaties gegevens gaat afleiden over gezondheidsgegevens zoals dyslexie, gaat het volgens het CBP om een verwerking van gevoelige gegevens (Onderzoek naar de verwerking van persoonsgegevens door Snappet, CBP rapport definitieve bevindingen van 14 juli 2014, p. 145). De beoordeling of de leerprestaties waaruit afgeleid kan worden of iemand aan dyslexie lijdt, daarmee ook op zichzelf al bijzondere persoonsgegevens zijn (met betrekking tot gezondheid) als bedoeld in artikel 16, jo. 21 van de Wbp, valt volgens het CBP echter buiten de scope van dit onderzoek.

Het is niet de eerste keer dat het CBP het begrip gevoelige gegevens in een oordeel naar voren brengt. In een rapport over de Smart TVs van Philips wordt bijvoorbeeld ook over gevoelige gegevens gesproken, terwijl het hier weer een heel ander soort gegevens betrof, namelijk gegevens over het kijkgedrag van volwassenen.

"TP Vision verzamelt gegevens over het onlinekijkgedrag, gebruik van apps en websitebezoek (op hoofddomein) van de gebruikers van Philips smart tv's, onder meer door middel van cookies, en bewaart deze. Ook verzamelt en bewaart TP Vision per smart tv wanneer er tv wordt gekeken, welke uitzendingen en apps favoriet zijn, elke uitzendingen een gebruiker opneemt, welke video's een gebruiker huurt en elke 'uitzending gemist'-uitzendingen een betrokkene bekijkt. Het CBP heeft vastgesteld dat deze gegevens persoonsgegevens zijn. Dit soort gegevens zijn 'gevoelige' persoonsgegevens. De gegevens over het onlinekijkgedrag, gebruik van apps en websitebezoek etc. kunnen een indringend beeld kunnen geven van iemands communicatiegedrag en soms ook iets zeggen over de inhoud van de communicatie." [onderstreping red.] (Onderzoek naar de verwerking van persoonsgegevens met of door een Philips smart tv door TP Vision Netherlands B.V., CBP rapport definitieve bevindingen van juli 2013, p. 2.).

In de Wbp komt het begrip "gevoelige persoonsgegevens" in het geheel niet voor. In Richtlijn 95/46 komt het begrip gevoelige gegevens evenmin voor. In artikel 16 worden bepaalde categorieën zeer gevoelige persoonsgegevens wel

aangemerkt als *bijzondere* persoonsgegevens, die alleen op basis van enkele specifieke grondslagen mogen worden verwerkt. Het gaat hier bijvoorbeeld om medische en strafrechtelijke gegevens. Daar vallen de gegevens van leerlingen in het kader van het gebruik van onderwijsapps echter niet onder. Wel worden kinderen tot 16 jaar extra beschermd doordat zij op grond van artikel 5 Wbp zelf geen toestemming kunnen geven voor het gebruik van hun persoonsgegevens, maar hun wettelijk vertegenwoordiger dat moet doen.

Ook Snappet merkt in haar zienswijze op dat de term gevoelige persoonsgegevens wettelijk niet gedefinieerd is. Volgens Snappet wordt de term door het CBP alleen maar gebruikt om een bepaald sentiment aan te wakkeren (Zienswijze Snappet als bijlage bij CBP rapport definitieve bevindingen van 14 juli 2014, p. 5). Volgens het CBP echter, onderscheidt de wetsgeschiedenis bij artikel 9 Wbp de begrippen 'bijzondere' en 'gevoelige' gegevens. Zij verwijst daarbij naar de volgende passage:

"Vervolgens is van belang de aard van de betreffende gegevens (onderdeel b). Artikel 16 betreft de gegevens die uit hun aard gevoelig zijn. Daarnaast kunnen gegevens gevoelig zijn door de context waarin zij worden gebruikt, bij voorbeeld de gegevens omtrent iemands kredietwaardigheid of welstand. Hoe gevoeliger het gegeven, hoe minder snel mag worden aangenomen dat er sprake is van verenigbaar gebruik indien bij enige verwerking wordt afgeweken van het oorspronkelijk doel." (*Kamerstukken II* 1997/98, 25 892, nr. 3, p. 90).

Dat is echter de enige keer in de Memorie van Toelichting dat de term gevoelige persoonsgegevens op deze manier wordt gebruikt. Voor het overige wordt de term gevoelige persoonsgegevens steeds gebruikt wanneer wordt gedoeld op de categorieën bijzondere persoonsgegevens als bedoeld in artikel 16 Wbp. Naar mijn mening kan hieruit dan ook niet worden afgeleid dat de wetgever een aparte categorie als zodanig in het leven heeft willen roepen, maar enkel dat in de context van artikel 9 rekening gehouden kan worden met de vraag of het om gegevens gaat die in meer of mindere mate gevoelig zijn.

Dat is ook logisch. De aard van persoonsgegevens speelt vanzelfsprekend een rol bij de afweging of sprake is van een verenigbaar doel, net als dat het geval is bij de belangenafweging die in het kader van artikel 8 sub f moet plaatsvinden, zoals ook in de Memorie van Toelichting is aangegeven.

"Bij de in onderdeel f voorgeschreven afweging speelt een rol de mate van gevoeligheid van de gegevens die de verantwoordelijke wil verwerken en de maatregelen die de verantwoordelijke heeft genomen ten einde rekening te houden met de belangen van de betrokkene. (*Kamerstukken II* 1997/98, 25 892, nr. 3, p. 88).

Waar de categorieën bijzondere persoonsgegevens uit artikel 16 dermate gevoelig zijn dat zij alleen op basis van specifieke grondslagen mogen worden verwerkt, geldt echter dat de mate van gevoeligheid van niet-bijzondere persoonsgegevens slechts één van de factoren is die bij de belangenafweging moet worden betrokken.

In de afweging van het CBP is het feit dat sprake is van gevoelige gegevens echter van doorslaggevende betekenis. Ten aanzien van de vraag of Snappet een beroep kan doen op artikel 8 sub f overweegt het CBP:

"Deze zes gegevensverwerkingen zijn niet evident noodzakelijk om onderwijs te kunnen geven met behulp van de tablets. Het feit dat de scholen ervoor kiezen om

een deel van het onderwijs via apps op de tablets te laten verlopen, en dat dat nieuwe technische mogelijkheden opent om persoonsgegevens te aggregeren, combineren en verder te verwerken, betekent nog niet dat dergelijke verwerkingen ook zonder meer toelaatbaar zijn. Het gaat hier deels om gevoelige persoonsgegevens, waaraan allerlei conclusies kunnen worden verbonden met gevolgen in het maatschappelijk leven. Gelet daarop voldoen de verwerkingen niet aan het proportionaliteitsvereiste."
(Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet, rapport definitieve bevindingen van 14 juli 2014, p. 50).

Dat is wel erg kort door de bocht. Als deze redenering wordt gevolgd, zouden gegevensverwerkingen die deels gevoelige gegevens betreffen nooit onder de grondslag van artikel 8 sub f kunnen vallen.

Het zou dan ook de voorkeur hebben als het CBP het begrip gevoelige gegevens niet langer zou gebruiken om een aparte categorie gegevens in het leven te roepen, maar de gevoeligheid van gegevens alleen als factor zou beschouwen bij de belangenafwegingen die in het kader van de Wbp moeten worden gemaakt. In de wet is immers al een afweging gemaakt van categorieën gegevens en betrokkenen die extra bescherming behoeven. Het toevoegen van niet gedefinieerde categorieën gevoelige gegevens die een doorslaggevende rol spelen voor de vraag of een gegevensverwerking is toegestaan, komt de rechtszekerheid niet ten goede.

V. Zwaan,