



Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens

Advies wetgeving VTC nr. 2022/115 van 17 januari 2023

over

tekst	Ontwerp van decreet
van	van de Vlaamse Regering
titel	Decreet over het onderwijs XXXIII
roepnaam	(OD XXXIII – leerID)
datum	zoals principieel goedgekeurd op 2 december 2022

De Vlaamse Toezichtcommissie (hierna "de VTC");

Gelet op het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (hierna: "het e-govdecreet"), inzonderheid artikel 10/4, §1;

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna AVG), inzonderheid artikel 36, 4, artikel 57, 1, c) en artikel 58, 3;

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna "WVG");

Gelet op het verzoek om advies van de heer Ben Weyts, Viceminister-president van de Vlaamse Regering en Vlaams minister van Onderwijs, Sport, Dierenwelzijn en Vlaamse Rand van 7 december 2022, ontvangen door de VTC op 7 december 2022;

Gelet op de behandeling op de zitting van 13 december 2022 en op de zitting van 17 januari 2023 en de beslissing om het dossier af te werken in een schriftelijke procedure;

Gelet op het overleg met vertegenwoordigers van de adviesvrager op 1 februari 2023;

Brengt op 17 januari 2023 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. De Vlaamse minister bevoegd voor Onderwijs en Vorming (hierna "de adviesvrager") verzocht om het advies van de Vlaamse Toezichtcommissie (hierna "VTC") over een voorontwerp van decreet over het onderwijs XXXIII (hierna "het Ontwerp"), zonder aanduiding van specifieke artikelen.

2. Aangezien de adviesbevoegdheid van de VTC op grond van artikel 10/4, § 1 van het e-govdecreet betrekking heeft op de verwerkingen van persoonsgegevens, is haar adviesverlening hiertoe beperkt.

Context

3. De nota aan de Vlaamse Regering geeft aan dat het Ontwerp drie doelstellingen beoogt te realiseren:

1. Een aanvulling en verbetering van een aantal bestaande decreten.

De artikelen in dit decreet bevatten een aantal technische correcties, verduidelijkingen en aanvullingen van bestaande thema- en niveaudecreten.

2. Een reeks maatregelen tot vereenvoudiging in zijn meest ruime zin.

Dit onderwijsdecreet (OD) gaat bijna uitsluitend om juridisch-technische verbeteringen of het in overeenstemming brengen van de onderwijsregelgeving onderling en met andere regelgeving.

3. Uitvoering geven aan de relanceplannen van de Vlaamse Regering

De nota verwijst naar de Visienota "Digisprong - Van Achterstand naar Voorsprong", het ICT-plan voor een kwalitatief digitaal onderwijs dat voortvloeit uit het relanceplan van de Vlaamse Regering "Vlaamse veerkracht". Deze visienota voorziet in het zgn. "LeerID". Meer concreet wordt actie 3.3. van Digisprong uitgevoerd, die luidt als volgt: "De toegang tot digitale leermiddelen vergemakkelijken via de **creatie van een "Single Sign On" infrastructuur**". Het LeerID wordt met dit decreet ingevoerd.

4. Enkel de uitwerking van de derde doelstelling lijkt relevant voor dit advies. Het Ontwerp wil in een **decretaale verankering voorzien voor het zgn. "LeerID"**.

5. De nota geeft volgende verduidelijking:

"LeerID is de single sign-on oplossing van de Vlaamse overheid, die leerlingen van het leerplichtonderwijs toelaat om via 1 gebruikersnaam en 1 wachtwoord aan te melden op allerhande digitale leermiddelen en toepassingen.

De LeerID moet een efficiëntere toegang tot digitale leermiddelen voorzien, een vermindering van administratief, handmatig en repetitief werk en planlast. De LeerID vormt tevens een veilig platform voor digitale toetsen, bijvoorbeeld de Vlaamse toetsen en garandeert een correcte afdekking van wettelijke vereisten zoals privacy en auteursrechten."

6. De artikelen 50 en 51 van het Ontwerp hebben betrekking op de leerID en de bijhorende verwerking van persoonsgegevens .

II. ONDERZOEK VAN DE ADVIESAANVRAAG

1. Voorafgaande toelichting

7. De VTC stelt vast dat de personen van wie gegevens worden verzameld en uitgewisseld de volgende zijn: de leerlingen die gebruik moeten maken van een leermiddel of de toepassing in het kader van hun onderwijs

en dat het minstens de volgende gegevens betreft: identificatiegegevens (zie verder voor volledig overzicht).

8. Het betreft informatie over natuurlijke personen met hun identificatiegegevens en dus gaat het om de verwerking van informatie over geïdentificeerde natuurlijke personen, zijnde persoonsgegevens zoals bedoeld in de AVG. De

VTC gaat daarom na in hoeverre het Ontwerp en de bestaande decreten in lijn liggen met de principes van het gegevensbeschermingsrecht.

9. De VTC wijst erop dat een single-sign-on systeem buiten gebruiksgemak een veiliger oplossing kan bieden dan de combinatie van verschillende aanmeldsystemen van diverse leveranciers. Aangezien echter unieke identificatie en authenticatie het makkelijker maken om personen – in casu leerlingen – te volgen over de verschillende systemen (en daaruit informatie over die leerlingen af te leiden), houdt dit een eigen risico inzake gegevensbescherming in. Unieke identificatie en authenticatie moeten dus beperkt blijven tot die toepassingen waarvoor ze noodzakelijk zijn. Anoniem gebruik maken van toepassingen moet het uitgangspunt blijven.

2. Beoordeling van de regelgevende grondslag

10. Met artikel 50 van het Ontwerp wordt er een hoofdstuk 5 “Unieke leerlingenaccounts” toegevoegd aan “de codificatie sommige bepalingen voor het onderwijs” van 28 oktober 2016¹.
11. Het komt de stellers van het Ontwerp toe om erover te waken dat – en dit ook voor de bestaande wet- en regelgeving – elke verwerking die in onderhavige context zal plaatsvinden een rechtvaardigingsgrond vindt in artikel 6 AVG.
12. Het Ontwerp vermeldt expliciet op grond van welke rechtvaardigingsgrond in de AVG de verwerking van persoonsgegevens zal plaatsvinden:

“§2. [...] De voormelde verwerkingsverantwoordelijke verwerkt de gegevens om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.”
13. Er wordt met dit decreet een verplichting ingevoerd om de informaticatoepassing aan te bieden.
14. De VTC wenst in herinnering te brengen dat elke overheidsinmenging in de bescherming van de persoonlijke levenssfeer zoals gewaarborgd door artikel 8 van het EVRM², artikel 7 van het Handvest van de Grondrechten van de Europese Unie samengelezen met artikel 52.1 van het Handvest en artikel 22 van de Grondwet moet worden voorgeschreven in een 'voldoende precieze wettelijke bepaling' die beantwoordt aan een dwingende maatschappelijke behoefte en evenredig is met de nagestreefde doelstelling. In een dergelijke precieze wettelijke bepaling moeten de essentiële elementen³ van de met de overheidsinmenging gepaard gaande verwerkingen van persoonsgegevens omschreven zijn.⁴

¹ [besluit van de Vlaamse Regering van 28 oktober 2016](#) betreffende de codificatie sommige bepalingen voor het onderwijs, bekrachtigd bij decreet van 23 december 2016, gewijzigd bij de decreten van 5 april 2019, 3 juli 2020, 9 juli 2021 en 25 februari 2022.

² Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden.

³ Artikel 6, AVG vermeldt de volgende elementen:

- het doel van de verwerking;
- de types of categorieën van te verwerken persoonsgegevens; Deze gegevens moeten bovendien beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking”);
- de betrokkenen;
- de entiteiten waaraan en doeleinden waarvoor de persoonsgegevens mogen worden verstrekt;
- de opslagperioden;
- de aanduiding van de verwerkingsverantwoordelijke(n).

⁴ EHRM, arrest *Rotaru c. Roumania*, 4 mei 2000; GWH 23 april 2015, arrest nr. 44/2015, 63; GWH 5 oktober 2017, arrest nr. 100/2017, 17; GWH 15 maart 2018, arrest nr. 29/2018, 26; GWH 14 januari 2021, arrest nr. 2/2021, overw. B.22.1.e.e.; GWH 18 november 2021, arrest nr. 158/2021, overw. B.6; GWH 9 december 2021, B.53.1-B.53.2; R.v.St, adv. 68.936/AV van 7 april 2021 over een voorontwerp van wet *betreffende maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie*, Parl.St. Kamer, 2020-2021, doc. nr. 551951/001, 94-98; SCHRAM, F., *Privacy & persoonsgegevens. Handboek*, Brussel, Politeia, 2019, 75-

15. Voor verwerkingen op basis van artikel 6, lid 1, c), AVG⁵, die niet zozeer betrekking hebben op het privé-leven, maar eerder enkel op de bescherming van persoonsgegevens, moet het doeleinde voldoende duidelijk afgebakend zijn⁶. Andere elementen van de verwerking die al duidelijk (eventueel impliciet) blijken uit de bestaande wetgeving moeten niet per se herhaald worden. De VTC vindt het niettemin een goede praktijk om dat wel te doen om een uniform kader te creëren waarop verschillende uitvoeringsbesluiten kunnen steunen. Bovendien maakt dit het veel gemakkelijker om de verwerkingen van persoonsgegevens te toetsen aan de AVG, zowel voor de toezichthouder als voor de betrokkenen. Er is dus een onderscheid te maken tussen de legaliteitstoets (eisen waaraan de wettelijke basis moet voldoen om geldig te zijn) en de conformiteitstoets aan de AVG.
16. Aangezien met de vermelding van de essentiële elementen ook minstens gedeeltelijk tegemoetgekomen wordt aan artikel 5, 1, a), AVG, dat bepaalt dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene behoorlijk en transparant is, zal het ontbreken van deze elementen zwaardere transparantiemaatregelen vragen. Er zal immers niet naar de wetgeving kunnen verwezen worden voor die elementen.
17. De opstellers van de wettelijke en reglementaire teksten zullen moeten inschatten of de beoogde verwerking een meer uitgewerkte rechtsgrond nodig heeft. Daarbij moet in eerste instantie gekeken worden naar de graad van inmenging van de overheid in het privé-leven.
18. Hierbij moet er op gelet worden dat in een eventueel uitvoeringsbesluit (mits delegatie aan de Vlaamse Regering) verdere modaliteiten kunnen worden bepaald, maar dat de essentie in het decreet zelf moet worden opgenomen, wat nu nog niet het geval is. De VTC verwijst naar de rechtspraak van het Grondwettelijk Hof inzake delegatie door de wetgever⁷)
19. In artikel 51 van het Ontwerp worden de essentiële elementen van de gegevensverwerking behandeld.

3. Doelbinding

20. Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (artikel 5, 1, b), AVG).
21. De volgende doeleinden worden in artikel 51 van het Ontwerp vermeld:

“Art. VI.10. §1. De Vlaamse Regering biedt een informaticoepassing aan, die tot doel heeft dat leerlingen zich kunnen identificeren om digitale leermiddelen en toepassingen te gebruiken waarvoor identificatie nodig is. Via de voormelde informaticoepassing melden leerlingen zich aan bij verschillende dienstenleveranciers met hetzelfde account. De school bepaalt welke leermiddelen of toepassingen de leerling moet gebruiken. De dienstenleveranciers vragen het gebruik van de informaticoepassing aan bij de verwerkingsverantwoordelijke, vermeld in paragraaf 2. “
22. In de toelichting wordt aangegeven dat door het toenemend gebruik van digitale leermiddelen en toepassingen in het onderwijs scholen worden geconfronteerd met heel veel leerlingenaccounts bij de verschillende dienstenleveranciers. Met het ontwerp kan de Vlaamse overheid een unieke oplossing aanbieden waarmee

98, 111-116; DEGRAVE, E., "L'é-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle", Collection du CRIDS, Larcier, Brussel, 2014, p. 161 e.v.

⁵ "c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;"

⁶ Artikel 6, 3, AVG. Voor wat punt e) betreft, bestaat de doelstelling van de verwerking in de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend door unierecht of lidstatelijk recht.

⁷ bv. GwH nr. 166/2011, 10 november 2011, overw. B.43.3 e.v., GwH nr. 158/2021, 18 november 2021, overw. B.8.4.2.

leerlingen bij verschillende dienstenleveranciers kunnen aanloggen op basis van één gebruikersnaam en één wachtwoord.

23. Dit wordt verder uitgewerkt op pagina 9 van de Toelichting (onderlijning VTC):

“Beleidsmaatregel 5. Leer-id

Door het gebruik van de LeerID zijn de effecten op kinderen en jongeren van minder dan 25 jaar onder meer:

Verbeterde toegang tot digitale leermiddelen en digitale toetsen;

Een meer veilige toegang tot digitale leermiddelen;

Gebruik en verwerking van persoonsgegevens met respect voor de privacy van het kind;

De LeerID zal de waarborg van het recht op onderwijs van al de kinderen en jongeren enkel maar versterken, ook van de meest kwetsbaren onder hen. Niet alleen zal de toegang tot digitale leermiddelen en digitale toetsen verbeterd worden, door de SSO-oplossing kunnen leerlingen net veiliger en op een meer uniforme manier aanloggen om meerdere digitale applicaties, daar waar nu aparte logins nodig zijn. Het gebruik van de LeerID verloopt bovendien via de school. De verwachting is immers dat zich de komende jaren een duidelijke groei van digitale toepassingen (leermiddelen, platformen, maar ook toetsen en evaluaties) zal doorzetten. Een eenvoudige, veilige toegangspoort ondersteunt het recht op kwaliteitsvol onderwijs.

Uiteraard worden leerlinggegevens verzameld omdat dit noodzakelijk is voor de goede werking van LeerID. LeerID gebruikt de Discimus-databank als voornaamste (en authentieke) bron van leerlinggegevens. Discimus is een databank ontwikkeld door het Agentschap voor Onderwijsdiensten en bevat registratiegegevens over alle leerlingen in het Vlaams onderwijs. Daarnaast verzamelt het Ministerie ook contactgegevens over de accounts die aangemaakt worden op LeerID. Kortom, het gebruik en verwerking van persoonsgegevens gebeurt met het maximale respect voor het recht op privacy van het kind of de jongere.

De 0-optie is dan ook geen optie. Indien de overheid geen eigen SSO-optie aanbiedt, is de verwachting dat commerciële spelers een eigen login zullen voorzien voor hun eigen applicaties. Los van de commerciële insteek is de overheid de enige speler die SSO oplossing voor alle leerlingen kan aanbieden. Een ander nadeel van de 0-optie is dat er voor diverse applicaties dan vaak aparte loginsystemen moeten gecreëerd worden, wat heel wat planlast en repetitief werk bij de al overbevraagde ICT-coördinatoren met zich meebrengt. Leerlingen dienen dan diverse logins bij te houden of te onthouden, wat de veilige toegang niet ten goede komt.
[...].”

24. De VTC beoordeelt het aanbieden van een single-sign-on oplossing in dit kader positief. Uit het Ontwerp en de toelichting blijkt ook dat het project een mogelijke opstap is naar de introductie van multifactorauthenticatie⁸ voor de leerlingen zoals die nu al geïntroduceerd wordt voor ouders en personeel.
25. De VTC wijst er wel op dat een zelfde login en paswoord gebruiken voor alle mogelijke toepassingen ook veiligheidsrisico's inhoudt. Zoals al gezegd, houdt unieke identificatie (en zeker authenticatie) ook privacyrisico's in want een leerling kan daarmee overmatig gevolgd worden over allerlei toepassingen en platformen heen. De adviesvragers hebben geantwoord dat dit opgevangen wordt doordat er bij elke aanmelding weer doorgestuurd wordt naar ACM/IDM. De meta gegevens volgend uit de registratie (wie wanneer welke applicatie gebruikt van waar) komen dus niet bij de leveranciers terecht (maar bij de beheerder van ACM/IDM).
26. Er moet dus blijvend over gewaakt worden dat het gebruik van single-sign-on beperkt blijft tot wat noodzakelijk is voor de werking binnen het schoolkader. Dit lijkt gewaarborgd door de bepaling “Art. VI.10. §1. *De Vlaamse Regering biedt een informaticatoepassing aan, die tot doel heeft dat leerlingen zich kunnen identificeren om digitale leermiddelen en toepassingen te gebruiken waarvoor identificatie nodig is.*”

⁸ Zie onder deel 5 i.v.m. gebruik INSZ.

4. Verantwoordelijkheid

27. Artikel 4.7) AVG bepaalt dat voor de verwerkingen waarvan de regelgeving het doel en de middelen vastlegt, de **verwerkingsverantwoordelijke** diegene is die daarin als dusdanig wordt aangewezen.
28. De tweede paragraaf van het nieuwe artikel VI.10 wijst de verwerkingsverantwoordelijke aan:
- “§2. De entiteit die door de Vlaamse Regering wordt belast met de voorbereiding van het Vlaamse onderwijsbeleid is verwerkingsverantwoordelijke als vermeld in artikel 4, 7), van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming).”*
29. Het Departement Onderwijs en Vorming is momenteel de entiteit belast met de voorbereiding van het Vlaamse onderwijsbeleid (Besluit van de Vlaamse Regering van 3 juni 2005 met betrekking tot de organisatie van de Vlaamse administratie, artikel 22 en 30).
30. De verwerkingsverantwoordelijke is dus voldoende duidelijk aangeduid voor de bedoelde verwerking.
31. Uit het overleg met de adviesvrager is wel gebleken dat de gegevens van de auditlogs en technische logs op termijn door de instantie die instaat voor het Vlaamse toegangs- en gebruikersbeheer zullen worden beheerd. Het is nog niet duidelijk of dit op basis van een verwerkersrelatie zal zijn of dat deze instantie hiervoor verwerkingsverantwoordelijke is. Zie hierna onder minimale gegevensverwerking.
32. De VTC heeft vernomen dat er een (of meer) gegevensbeschermingsimpactanalyse(s) werden gemaakt die aan haar zal(zullen) worden voorgelegd.

5. Minimale gegevensverwerking

33. Conform artikel 5.1, c), AVG, moeten de persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.
34. De **categorieën betrokkenen** worden aangeduid in § 5 van het nieuwe artikel VI.10:
- “§5. De betrokkenen zijn de leerlingen die het leermiddel of de toepassing moeten gebruiken in het kader van hun onderwijs.[...].”*
35. De **categorieën persoonsgegevens** worden aangeduid in § 4 van het nieuwe artikel VI.10.
- 1° het identificatienummer van de sociale zekerheid;
 - 2° de volgende officiële persoonsgegevens: de voor- en achternaam, het geslacht en de geboortedatum;
 - 3° de unieke identificator voor de informaticatoepassing;
 - 4° de unieke identificator in de administratieve gegevens die beschikbaar zijn bij de entiteiten van het beleidsdomein Onderwijs en Vorming, vermeld in artikel 7 van het besluit van de Vlaamse Regering van 3 juni 2005 met betrekking tot de organisatie van de Vlaamse administratie;
 - 5° de inschrijvingsdatum en de begindatum;
 - 6° de volgende inschrijvingsgegevens: de instellingen, het vestigingsplaatsnummer, het stamnummer, het soort onderwijs en de administratieve groep;

7° de accountgegevens.

36. In de memorie van toelichting wordt de volgende motivering gegeven bij deze categorieën (onderlijning VTC):

“Paragraaf 4 bepaalt welke gegevens noodzakelijk zijn voor de informaticatoepassing. Het INSZ-nummer wordt enkel gebruikt voor toekomstige veiligere manieren van authenticeren (Multifactor Authenticatie) en enkel uitgeleverd aan de dienstenleveranciers als ze over een decretale basis beschikken voor verwerking van dat nummer. Naam, voornaam, geslacht, geboortedatum, zijn nodig om de regels rond paswoordsterkte te bepalen. Enkel naam en voornaam worden uitgeleverd aan de dienstenleveranciers. De unieke identificator voor de informaticatoepassing is nodig voor de authenticatie van de leerling in de aansluitende platformen. De unieke identificator in de beschikbare gegevens is nodig voor eventuele koppeling met de unieke identificator voor de informaticatoepassing. De datum waarop de leerling ingeschreven en gestart is in een school is nodig om de meest actuele gegevens te hebben. Gegevens over de instelling(en), vestigingsplaatsnummer, stamnummer, soort onderwijs en administratieve groep zijn nodig om de leerling in de juiste school te kunnen weergeven en de beheerder toe te laten de leerlingen van zijn school eenvoudig op te zoeken. De accountgegevens zijn nodig om de dienstenleverancier de informaticatoepassing te laten gebruiken.”

37. De VTC ziet niet in waarom het gegeven geslacht noodzakelijk is om regels over paswoordsterkte te bepalen. Ze beveelt aan om dit gegeven te schrappen.

38. De uitdrukking “officiële persoonsgegevens” is niet geheel duidelijk. Waarschijnlijk worden identificatiegegevens bedoeld zoals die in de Discimustoeppassing zijn opgenomen of de rijksregistergegevens? De VTC adviseert om dit te verduidelijken.

39. Ze wijst er ook op dat wat het INSZ betreft, het gebruik van het bisnummer vrij is en dat de leveranciers in principe als verwerker kunnen steunen op de rechtvaardigingsgrond(en) van de onderwijsinstelling voor wie ze persoonsgegevens verwerken.

40. De term “accountgegevens” is ook onvoldoende duidelijk en ingeperkt en de VTC adviseert dat deze in de eerste plaats in het Ontwerp zelf verduidelijkt wordt.

41. Aan de Vlaamse Regering wordt in dezelfde paragraaf de mogelijkheid gegeven de vermelde categorieën van persoonsgegevens nader te omschrijven. De VTC ziet niet onmiddellijk wat er verder nog verduidelijkt kan worden (wat niet in het decreet zelf behoort te gebeuren op basis van de opmerkingen hiervoor gegeven). Dit zou kunnen aangegeven worden in de toelichting.

42. De VTC is van oordeel dat er voor het overige voldaan wordt aan het principe van minimale gegevensverwerking onder voorbehoud van wat in de inleiding al gesteld werd inzake de loggegevens die informatie geven over wie, wanneer en eventueel van waar toegang had tot een bepaalde applicatie.

43. Wat de **ontvangers** betreft: paragraaf 5 verduidelijkt wie de ontvangers van de gegevens zijn:

“§5. [...] De dienstenleveranciers zijn ontvangers van de gegevens die noodzakelijk zijn voor het doel van de identificatie van gebruikers of de controle van de gebruiksvoorwaarden.”

44. De toelichting verduidelijkt dat de dienstenleveranciers enkel de gegevens ontvangen die nodig zijn voor de identificatie van gebruikers of de controle van de gebruiksvoorwaarden (bijvoorbeeld leerling van een school die de toepassing mag gebruiken).

45. Hiervoor werd al uit de toelichting geciteerd (zie randnummer 36) dat enkel naam en voornaam worden uitgeleverd aan de dienstenleveranciers. De VTC adviseert dat verder wordt bepaald welke gegevens juist naar deze private actoren gaan en dit bij voorkeur in het Ontwerp zelf.

46. De leveranciers treden zoals gezegd op als verwerkers voor de onderwijsinstellingen. Deze laatste beschikken al over deze gegevens die ze zelf aan de onderwijsadministratie hebben bezorgd.

47. Paragraaf 3 verduidelijkt dat in het kader van de eenmalige gegevensopvraging de informaticatoepassing gegevens gebruikt die al beschikbaar zijn bij het onderwijsministerie:

“§3. De verwerkingsverantwoordelijke, vermeld in paragraaf 2, gebruikt in de informaticatoepassing, vermeld in paragraaf 1, administratieve gegevens die beschikbaar zijn bij de entiteiten van het beleidsdomein Onderwijs en Vorming, vermeld in artikel 7 van het besluit van de Vlaamse Regering van 3 juni 2005 met betrekking tot de organisatie van de Vlaamse administratie, conform de regelgeving over de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens die van toepassing is bij de mededeling van persoonsgegevens, zoals ze in voorkomend geval op federaal of Vlaams niveau verder is of wordt gespecificeerd.”

48. Krachtens artikel 5.1, e) AVG mogen persoonsgegevens niet langer worden **bewaard**, in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt.

49. De zesde paragraaf van het Ontwerp legt de bewaartermijn vast:

“§6. De gegevens worden door de verwerkingsverantwoordelijke niet langer bewaard dan twaalf jaar.[...]”

50. De adviesvrager heeft in een overleg toegelicht dat deze termijn enerzijds gebaseerd is op de standaard termijn voor het bijhouden van loggegevens door de Vlaamse overheid en anderzijds door de in regel 12-jarige schoolloopbaan. De VTC acht het noodzakelijk dat de aanvang deze termijn wordt bepaald in het Ontwerp en dat de termijn verantwoord wordt in de toelichting. Zij kan de proportionaliteit nu onvoldoende beoordelen.

6. Juistheid

51. Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd (artikel 5, 1, d), AVG).

52. Het Ontwerp bevat volgende bepaling hierover:

§6 [...]De verwerkingsverantwoordelijke, vermeld in paragraaf 2, neemt de nodige maatregelen om de juistheid van de persoonsgegevens te garanderen.”

53. De VTC is van oordeel dat dit hier volstaat.

7. Rechten van de betrokkenen en transparantie

54. Artikel 12 AVG bepaalt dat de verwerkingsverantwoordelijke passende maatregelen neemt opdat de betrokkene de in de artikelen 13 en 14, AVG bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34, AVG bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt.

55. De zesde paragraaf van het nieuwe artikel VI.10 legt het volgende op:

“§6 [...]De verwerkingsverantwoordelijke, vermeld in paragraaf 2, verduidelijkt in een privacyverklaring welke verwerkingen er gebeuren en neemt met het oog op transparantie en de garantie van de rechten van betrokkenen, vermeld in paragraaf 5, in de communicatie naar de voormelde betrokkenen of hun onderwijsinstelling een verwijzing op naar de vindplaats van de privacyverklaring.”

56. De VTC beoordeelt deze handelswijze als voldoende onder voorbehoud van wat hierna gesteld wordt.

8. Beveiligingsmaatregelen

57. Artikel 32 AVG verplicht de verwerkingsverantwoordelijke om gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau verzekeren rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.

58. De VTC wijst erop dat aangezien de toepassing de toegang van de leerlingen tot de diverse leerplatform zal bepalen en aangezien het ook kinderen betreft, een bijzondere aandacht vereist is inzake informatieveiligheid.

59. Artikel 32, AVG wijst op een aantal voorbeeldmaatregelen om, waar passend, een op het risico afgestemd beveiligingsniveau te waarborgen:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingsystemen te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

60. Voor de concrete uitwerking hiervan wijst de VTC op de aanbeveling⁹ ter voorkoming van gegevenslekken en op de referentiemaatregelen¹⁰ die bij elke verwerking van persoonsgegevens in acht zouden moeten worden genomen. De VTC benadrukt ook het belang van een behoorlijk gebruikers- en toegangsbeheer¹¹ en een logging van de toegangen zodat de functionaris en de toezichhouders kunnen controleren wie wanneer toegang had tot welke gegevens, wat zijn/haar acties waren en waarom¹². De VTC verwijst naar de richtlijnen die ze gepubliceerd heeft voor het gebruik van digitale middelen voor scholen¹³.

61. Voor zover er gedacht wordt aan het gebruik van cloudtoepassingen, verwijst de VTC naar haar adviezen en aanbevelingen daarover¹⁴.

62. In geval beroep wordt gedaan op een verwerker dan wijst de VTC op volgende vereisten::

- sluiten van een verwerkersovereenkomst;
- aanstellen van een DPO door de verwerker;
- aanwijzen van categorieën personen die toegang hebben en lijst bijhouden.

⁹ Aanbeveling CBPL nr. 01/2013

(<https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2013.pdf>)

¹⁰ Referentiemaatregelen CBPL voor de beveiliging van elke verwerking van persoonsgegevens, Versie 1.0 (<https://www.gegevensbeschermingsautoriteit.be/publications/nota-inzake-de-beveiliging-van-persoonsgegevens.pdf>)

¹¹ Zie ook Aanbeveling CBPL nr. 01/2008

(<https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2008.pdf>)

Verschillende instanties kunnen hiervoor aangepaste technologische oplossingen bieden (zoals bijvoorbeeld de Kruispuntbank van de Sociale zekerheid).

¹² *Audit trailing of beveiligd controlespoor.*

¹³ Richtlijnen van de Vlaamse Toezichtcommissie bij het gebruik van digitale middelen in het onderwijs zoals leerlingen, cursisten- en personeelsadministratie, leerlingvolgsystemen, pakketten voor financieel beheer, educatief lesmateriaal en elektronische leeromgevingen,... (<https://overheid.vlaanderen.be/advies-rtc-nr-2020/01>)

¹⁴ <https://overheid.vlaanderen.be/vlaamse-toezichtcommissie-cloud>

63. De VTC beveelt aan dat in het Ontwerp de verplichting wordt opgenomen om een beheersstructuur of -procedure op te zetten om de leveranciers voor hun aansluiting op het systeem en tijdens de uitvoering te kunnen beoordelen.
64. In principe moet de specificering van maatregelen niet in de wetgeving worden opgenomen. Wanneer de decreetgever of in een later stadium (mits delegatie), de Vlaamse Regering echter vermoedt dat de gepaste maatregelen niet gerealiseerd zullen worden zonder dit aan de betrokken instanties expliciet op te leggen, dan moet dat wel gebeuren¹⁵.
65. De VTC verwijst naar haar **advies VTC/A/P/2022/05**¹⁶ over een ontwerpprotocol waarin een aantal verbeterpunten voor de praktische uitwerking werden voorgesteld.
66. De VTC beveelt aan om **in de communicatie** met de kinderen en de ouders het principe van de single-sign-on te verduidelijken en tegelijk uit te leggen waarom single-sign-on (gebruik zelfde wachtwoord en unieke identificatie) in deze context wel wenselijk of aanvaardbaar is, maar niet voor alle andere mogelijke toepassingen. De VTC adviseert ook om goede instructies te geven m.b.t. het aanmaken van een robuust wachtwoord.

III. BESLUIT

67. De VTC is van oordeel dat het voorgelegde voorontwerp dient grondig aangepast te worden, met nadruk op volgende elementen:
- het gegeven geslacht schrappen (luik 5 van dit advies);
 - "officiële" gegevens verduidelijken (luik 5);
 - de verwijzing naar het INSZ aanpassen (luik 5);
 - verduidelijken wat "accountgegevens" inhoudt (luik 5);
 - preciseren welke gegevens aan de verwerkers worden bezorgd;
 - in het Ontwerp de verwerking van de loggegevens behandelen;
 - verduidelijken dat er een essentieel verschil is tussen "identificeren" en "authenticeren": de ID op zichzelf laat geen authenticatie toe, hoewel dit gesuggereerd wordt in de vermelde toepassingen zoals "testen op afstand" (luik 5);
 - de delegatie aan de Vlaamse Regering herbekijken (luik 5);
 - de bewaartermijn verder preciseren en motiveren (luik 5);
 - de transparantiemaatregelen verder uitwerken (luik 7 en 8);
 - een beheerssysteem/procedure opzetten voor de aansluiting van de leveranciers (luik 8);
 - de introductie van het single-sign-on systeem te ondersteunen door awareness training en begeleiding (luik 8).

Hans Graux,
Voorzitter VTC

Getekend door: Hans Graux (Signature)
Getekend op: 2023-02-13 18:05:58 +01:00
Reden: Ik keur dit document goed



¹⁵ Dit kan eventueel ook in een ministerieel besluit of een omzendbrief.

¹⁶ https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_A_P_2022_05_advies_protocol.pdf