Bijlagen 1 t/m 3 bij de Model Verwerkersovereenkomst 4.0

Verwerker: Puzzel.org

Deze bundel bevat de drie bijlagen die de Verwerker invult bij de Model Verwerkersovereenkomst 4.0 van het Convenant Digitale Onderwijsmiddelen en Privacy. Bijlage 4 wordt door de Onderwijsinstelling zelf ingevuld en is hier niet opgenomen.

MODEL BIJLAGE 1: PRIVACYBIJSLUITER Puzzel.org

A. Contactgegevens

Voor vragen of opmerkingen over deze Privacybijsluiter of de werking van dit product en/of deze dienst, kunt u terecht bij:

	Functie en naam contactpersoon	Contactgegevens
Verwerker	Eigenaar en enig contactpersoon — Daan Weustenraad	daan@puzzel.org Er wordt geen telefoonnummer gepubliceerd; contact verloopt per e-mail.
Onderwijsinstelling*	[In te vullen door de Onderwijsinstelling]	[In te vullen door de Onderwijsinstelling]

* Deze contactpersoon is bevoegd/gemandateerd om namens de Onderwijsinstelling opdrachten en Instructies aan de Verwerker te verstrekken.

B. Versienummer en versiedatum

Verwerker: **Puzzel.org**. Versienummer **1.3**, versiedatum **25 september 2026**.

C. Algemene informatie (in te vullen door Verwerker)

Veld	Invulling
Naam product en/of dienst	Puzzel.org
Naam Verwerker en vestigingsgegevens	Puzzel.org, Sneekermeer 13, 3825XT Amersfoort, Nederland. KvK-nummer 66090091, btw-nummer NL002191535B44. Puzzel.org — eenmanszaak, ingeschreven in het Handelsregister van de Kamer van Koophandel onder nummer 66090091
Link naar Leverancier (website/URL)	https://puzzel.org
Link naar productpagina (website/URL)	https://puzzel.org/nl — overzicht van de activiteitentypen: https://puzzel.org/nl/activities — leveranciersinformatie voor ICT-afdelingen: https://puzzel.org/nl/vendor-info

Veld	Invulling
Beknopte uitleg en werking product en/of dienst	Puzzel.org is een webapplicatie waarmee een docent interactieve leeractiviteiten maakt — kruiswoordpuzzels, woordzoekers, quizzen, memory, escaperoom-achtige opdrachten en nog ruim dertig andere typen (36 activiteitstypen in totaal) — en die deelt met leerlingen via een link, een QR-code, een deelnamecode, een insluitcode (embed) of de eigen elektronische leeromgeving van de school. Er is geen installatie: alles draait in de browser. Standaard speelt een leerling anoniem en wordt er niets over de leerling vastgelegd. Een docent kan per activiteit twee afzonderlijke instellingen aanzetten: resultaten bijhouden en registratie verplichten. Pas dan worden er persoonsgegevens van leerlingen verwerkt, en alleen de velden die de docent zelf uit een vaste lijst kiest.
Doelgroep (po/vo/(v)so/mbo)	po, vo, (v)so en mbo. Het product is niet tot een sector beperkt en wordt ook in het hoger onderwijs gebruikt; dat valt buiten het Convenant.
Gebruikers (Onderwijsdeelnemers/ouders/verzorgers/medewerkers)	Onderwijsdeelnemers en medewerkers van de Onderwijsinstelling. **Ouders/verzorgers zijn geen gebruikers**: het platform kent geen ouderrol, geen ouderaccount en geen oudercommunicatie.

D. Omschrijving specifieke producten en/of diensten (in te vullen door Verwerker)

D.1 Producten en/of diensten en bijbehorende Verwerkingen die een onlosmakelijk onderdeel vormen van het aangeboden product en/of de aangeboden dienst

Omschrijving product en/of dienst	Bijbehorende Verwerking(en)
1. Docentaccount en inloggen	Aanmaken en beheren van een account voor een medewerker van de Onderwijsinstelling: voornaam, e-mailadres en taalvoorkeur. Inloggen met e-mailadres en wachtwoord, of met het Google- of Microsoft-account dat de school al beheert. Authenticatie loopt via Google Firebase Authentication; het wachtwoord wordt door Firebase beheerd en komt niet in de database van Puzzel.org. Koppeling met derde partij: Google Firebase Authentication (en, bij SSO, de identiteitsprovider van de school).
2. Activiteiten maken, opslaan en beheren	Opslaan van de inhoud die de docent maakt: vragen, antwoorden, aanwijzingen, teksten, instellingen, mappen en sjablonen. Deze inhoud is door de docent vrij in te vullen ("open velden") en kan daardoor persoonsgegevens bevatten die de Verwerker niet vooraf kan begrenzen.
3. Bestanden uploaden	Opslaan van afbeeldingen, geluidsfragmenten en documenten die de docent uploadt, in Amazon S3, onder een sleutel waarin het account-id van de docent is opgenomen. **Let op: geüploade bestanden krijgen een publiek leesbare URL.** Wie de URL heeft, kan het bestand opvragen. Geüploade documenten (PDF) worden vóór publicatie in quarantaine op malware gecontroleerd.
4. Een activiteit spelen	Een speler wordt — ook zonder account — anoniem aangemeld bij Firebase Authentication, zodat de applicatie een tijdelijk speler-id heeft. Zonder de optionele diensten onder D.2 worden er geen gegevens over de speler opgeslagen: geen naam, geen score, geen resultaat. Voortgang binnen één sessie blijft in de browser.
5. Beveiliging en misbruikpreventie	Snelheidsbegrenzing (rate limiting) op publieke eindpunten, op basis van het speler-id en van een **met een geheim gezouten SHA-256-hash van het IP-adres**; het IP-adres zelf wordt niet opgeslagen. Tellen van het aantal spelsessies per maand voor de abonnementslimiet.

Omschrijving product en/of dienst	Bijbehorende Verwerking(en)
6. Beschikbaarheid, onderhoud en ondersteuning	Hosting en levering van de applicatie via Vercel; opslag en beheer van de gegevens in Google Firebase Realtime Database; e-mail aan de accounthouder over het account en over storingen via SendGrid; ondersteuning per e-mail via daan@puzzel.org.
7. Weblettertypen	Elke pagina — **ook een spelpagina die een leerling opent** — laadt de lettertypen vanaf de eigen omgeving van Puzzel.org. De lettertypebestanden horen bij de applicatie en worden vanaf hetzelfde domein geserveerd; er wordt geen externe lettertypedienst aangesproken en er bereikt geen enkel gegeven over de bezoeker zo'n dienst. Tot 20 september 2026 kwamen de lettertypen van Google Fonts; die verbinding is verwijderd.

D.2 Aanvullende optionele producten en/of diensten en bijbehorende Verwerkingen die de Verwerker aanbiedt

In de laatste kolom kruist de Onderwijsinstelling aan of deze akkoord gaat met de aanvullende optionele producten en/of diensten en bijbehorende Verwerking(en). Elke dienst hieronder staat standaard **uit** en wordt alleen actief doordat de docent of de school hem aanzet.

Omschrijving product en/of dienst	Bijbehorende Verwerking(en)	Akkoord van de Onderwijsinstelling
8. Resultaten bijhouden (standaard uit)	Vastleggen per speler van: het tijdstip van spelen, de bestede tijd, de voortgang, de gegeven antwoorden, welke antwoorden goed waren, een eventuele score en het aantal pogingen. Het resultaat wordt opgeslagen onder het account van de docent, per activiteit en per speler. Een speler kan uitsluitend het eigen resultaat lezen; de docent leest alle resultaten van de eigen activiteit.	☐
9. Registratie van spelers (standaard uit)	De speler vult vóór of na het spelen een formulier in. De docent kiest zelf welke velden worden gevraagd uit deze vaste lijst: naam, voornaam, achternaam, e-mailadres, telefoonnummer, leerlingnummer, medewerkersnummer, organisatienaam, klas, land, "overige informatie", wachtwoord en één zelf geformuleerde vraag. Standaard wordt alleen om een voornaam gevraagd. Activiteiten die vóór 26 augustus 2026 zijn gemaakt, dragen nog de oudere standaardselectie naam, e-mailadres en wachtwoord. In beide gevallen bepaalt de docent de uiteindelijke selectie. De velden "overige informatie" en de zelf geformuleerde vraag zijn open velden. **Let op:** kiest de docent het veld *wachtwoord*, dan maakt de leerling een echt, blijvend gebruikersaccount aan bij Firebase Authentication mét een eigen accountrecord bij Puzzel.org (voornaam, e-mailadres, taalvoorkeur). Bij de overige velden blijft de speler anoniem. Het ingevoerde wachtwoord wordt niet in het resultaat opgeslagen.	☐
10. Klassikale ranglijst (standaard uit)	Tonen van spelers met hun tijd of score aan andere spelers van dezelfde activiteit. De ranglijst is een afgeschermde weergave: er wordt uitsluitend één naamveld gepubliceerd, en is dat een e-mailadres of telefoonnummer, dan wordt het gemaskeerd. Het volledige registratieformulier komt er niet in.	☐
11. Single sign-on voor spelers (standaard uit)	De speler meldt zich aan met een Google- of Microsoft-account, vanuit een eigen portaal van de school, of via OIDC tegen een per account toegelaten uitgever. Het account-id, en afhankelijk van de instelling de naam en het e-mailadres, worden bij het resultaat bewaard.	☐

Omschrijving product en/of dienst	Bijbehorende Verwerking(en)	Akkoord van de Onderwijsinstelling
12. Puzzel LMS — klassen en cursussen	Vastleggen van een klassenlijst onder het account van de docent: per leerling voornaam, optioneel achternaam, optioneel e-mailadres, een volgorde, een hash van een zelfgekozen wachtwoord en, na aanmelden met SSO, de provider en het e-mailadres van dat account. Dit is de enige verwerking waarin een echte klassenlijst bij de Verwerker wordt opgeslagen. Cursussen kunnen documenten en video's van de docent bevatten. Per leerling per activiteit kan de docent een eigen score (0–100%) en een opmerking vastleggen; de leerling ziet die bij de activiteit in de cursus. Bij het kiezen van een naam uit de klassenlijst en bij "niet jij?" wordt vastgelegd welke naam op welk apparaat werd gekozen of vrijgegeven: een willekeurig apparaat-id dat de browser zelf aanmaakt, een grove apparaataanduiding (browser en soort apparaat, bijvoorbeeld "Safari · iPad") en het tijdstip — geen IP-adres. Alleen de docent ziet dit naamwissel-logboek, zodat die kan zien of een leerling onder de naam van een klasgenoot speelt; het wordt na 30 dagen automatisch verwijderd. Een leerling kan in een cursus werk inleveren: een geschreven tekst, foto's en PDF's, met een optionele opmerking voor de docent. Foto's worden vóór het uploaden in de browser opnieuw getekend, waardoor metadata zoals de locatie verdwijnen; PDF's worden vóór publicatie op malware gecontroleerd. De bestanden staan in Amazon S3 in de bestandsregio van de docent, in een map per leerling, onder een openbaar leesbare URL die niet te raden is. Stuurt de docent werk terug ter verbetering, dan blijft de ingeleverde versie — tekst, bestanden, opmerking en de score en opmerking van de docent — bewaard als geschiedenis van dat werk. **Leerlingaccounts (optioneel; staat voor een Onderwijsinstelling uit tot zij die aanzet).** In plaats van een klassenlijst per klas kan de Onderwijsinstelling één leerlingenlijst bijhouden, per leerling met een e-mailadres, en elke leerling één account geven voor al zijn of haar klassen. De leerling krijgt via SendGrid één e-mail met een eenmalige link, zeven dagen geldig, om een wachtwoord te kiezen; dezelfde e-mail dient om het wachtwoord opnieuw in te stellen. Per leerling worden opgeslagen: de gegevens van de klassenlijst hierboven, een hash van het wachtwoord, de aanmeldmethode en het tijdstip van de laatste aanmelding. Klassen zonder leerlingaccounts werken zoals hierboven beschreven.	☐
13. Cijferkoppeling met Google Classroom	De docent verbindt het eigen Google-account. Opgeslagen worden: het Google-account-id en het e-mailadres van de docent, de verleende rechten en een versleuteld vernieuwingstoken; de sleutel waarmee dat token is versleuteld blijft op de server. Per opdracht en per leerling: het Google-account-id van de leerling, het id van de inzending, het laatst verzonden cijfer en het tijdstip. Naar Google worden verzonden: de opdrachtgegevens (titel, omschrijving, de link naar de activiteit, het maximumaantal punten, de inleverdatum) en het **cijfer** van de leerling. De gevraagde rechten zijn beperkt tot: het lezen van de cursussen van de docent, het beheren van leerlinginzendingen bij opdrachten, en het e-mailadres van het verbonden account; er wordt **geen** klassenlijst opgehaald.	☐
14. Cijferkoppeling via LTI 1.3 met de eigen leeromgeving (Moodle, Canvas, Brightspace en vergelijkbaar)	Bij het starten van een activiteit vanuit de leeromgeving ontvangt Puzzel.org uit het ondertekende identiteitsbericht van het platform: het platform-id van de gebruiker, en voor zover de school die deelt de naam en het e-mailadres, plus de rol. Er wordt geen Puzzel.org-account voor de leerling aangemaakt. Als de docent cijfers laat terugschrijven, worden per leerling het platform-id, het adres van de cijferkolom en het laatst verzonden cijfer bewaard, en wordt alleen het **cijfer** naar het platform verzonden.	☐

Omschrijving product en/of dienst	Bijbehorende Verwerking(en)	Akkoord van de Onderwijsinstelling
15. Deelnemen met een code (join-PIN)	Een activiteit krijgt een tijdelijke cijfercode die naar de gewone speel-URL verwijst. Opgeslagen wordt uitsluitend de koppeling tussen de code en de activiteit; er wordt niets over de intypende leerling vastgelegd. De code verloopt en wordt door een dagelijkse taak opgeruimd.	☐
16. Schoolaccount en gedeelde bibliotheek	Meerdere docenten werken onder één schoolaccount. Vastgelegd worden de koppeling tussen de docent en de school en, bij een gedeelde bibliotheek, een tijdelijk bewerkingsslot dat aangeeft wie een activiteit op dat moment bewerkt.	☐
17. AI-assistent voor de docent	Wat de docent intypt of uploadt wordt naar een externe AI-aanbieder gestuurd om inhoud te laten genereren. **OpenAI** ontvangt vrije tekst: een thema, een opsomming van antwoorden, of — bij het vertalen van een activiteit — de volledige tekst van die activiteit (tot circa 120.000 tekens). **Google Gemini** ontvangt afbeeldingen en volledige documenten: een geüploade PDF, Word-bestand of foto van een werkblad waaruit opgaven worden gedestilleerd, en afbeeldingen die bewerkt moeten worden. Als een docent een werkblad of een foto uploadt waarop persoonsgegevens staan, gaan die mee. De vraag en het antwoord worden ook onder het account van de docent bewaard.	☐
18. Woordcontrole tijdens het spelen (alleen bij het activiteitstype "wordle")	Wanneer een leerling bij dit ene activiteitstype een woord raadt dat niet in de antwoorden van de activiteit en niet in de meegeleverde woordenlijst staat, wordt **het door de leerling ingetypte woord** naar OpenAI gestuurd met de vraag of het een bestaand woord is. Het speler-id gaat niet mee; OpenAI ontvangt alleen het losse woord en de taalcode. De invoer is technisch begrensd tot één woord van uitsluitend letters, en een eerder gecontroleerd woord wordt uit een tijdelijke opslag beantwoord zonder OpenAI te raadplegen. **Dit is de enige verwerking waarbij door een leerling ingevoerde inhoud het platform verlaat richting een AI-aanbieder.** De Onderwijsinstelling kan dit uitsluiten door het activiteitstype "wordle" niet te gebruiken.	☐
19. Publiceren in de openbare activiteitenbibliotheek	De docent publiceert een activiteit voor hergebruik door anderen. Alleen de inhoud van de activiteit wordt gepubliceerd; resultaten, registraties, voortgang en instellingen voor tracking, multiplayer en ontwikkelaars worden nooit meegekopieerd.	☐
20. Betaald abonnement	Voor een betaald abonnement worden het e-mailadres van de accounthouder en het account-id aan Stripe doorgegeven en worden factuurgegevens van de instelling vastgelegd (naam, adres, postcode, plaats, land, btw-nummer). Betaalkaartgegevens worden uitsluitend door Stripe verwerkt en bereiken de systemen van Puzzel.org niet.	☐
21. Openbare API	Een account kan met een sleutel activiteiten aanmaken vanuit eigen systemen, maximaal 10 verzoeken per dag per sleutel.	☐
22. Wijzigen van de opslagregio	Het verplaatsen van alle accountgegevens naar de andere regio (zie onderdeel G) draait als achtergrondtaak en vereist een betaald abonnement.	☐

E. Doeleinden voor het verwerken van Persoonsgegevens

Verwerking van Persoonsgegevens met behulp van Digitale Onderwijsmiddelen door Onderwijsinstellingen vindt plaats ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van

het onderwijs(proces) en het begeleiden en volgen van Onderwijsdeelnemers (in hun leerproces). Hieronder staat aangegeven welke meer specifieke doeleinden van toepassing zijn op het product of de dienst.

Doeleinde	**Aankruisen indien van toepassing op product of dienst**
de opslag van leer- en toetsresultaten	☒
het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten	☒
de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer	☐
analyse en interpretatie van leer- en toetsresultaten	☒
het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen	☒
de indeling en aanpassing van roosters	☐
het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs	☐
het begeleiden en ondersteunen van leerkrachten/docenten en andere medewerkers binnen de Onderwijsinstelling	☐
de communicatie met Onderwijsdeelnemers en ouders en met medewerkers van de Onderwijsinstelling	☒
monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs	☐
het voor zover noodzakelijk en wettelijk toegestaan uitwisselen van Persoonsgegevens met Derden, waaronder: toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak; samenwerkingsverbanden in het kader van passend onderwijs en regionale samenwerkingen; partijen betrokken bij de invulling van stage- of leer-werkplekken; het leveren van Persoonsgegevens aan Onderwijsinstellingen in geval van overstappen tussen Onderwijsinstellingen en bij vervolgonderwijs; het in opdracht van de Onderwijsinstelling leveren van Persoonsgegevens aan een andere partij	☐
het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier	☒
het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie	☒
de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens	☒
de continuïteit, verbetering, goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning	☒
het door de Onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek	☐
het door de Onderwijsinstelling voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren	☐

Doeleinde	Aankruisen indien van toepassing op product of dienst
het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen	☐
het behandelen van geschillen	☐
financieel beheer	☒
de uitvoering of toepassing van een Unierechtelijke of lidstaatrechtelijke wettelijke bepaling of regeling	☐
andere doeleinden ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van Onderwijsdeelnemers (in hun leerproces), namelijk …	☐

Toelichting bij de aangekruiste doeleinden.

- *Opslag, terugontvangen, analyse en uitwisseling van leer- en toetsresultaten* zijn aangekruist omdat de optionele diensten 8, 13 en 14 daarin voorzien: resultaten worden opgeslagen, zijn door de docent in te zien en te exporteren, en een behaald cijfer kan worden teruggeschreven naar Google Classroom of naar de leeromgeving van de school. Zonder die opties wordt er niets opgeslagen.
- *Communicatie* betreft medewerkers, en een leerling alleen als de Onderwijsinstelling leerlingaccounts aanzet (dienst 12): de leerling krijgt dan één e-mail om een wachtwoord te kiezen, die ook dient om het opnieuw in te stellen. De ranglijst (dienst 10) toont spelers aan elkaar binnen dezelfde activiteit.
- *Financieel beheer* betreft uitsluitend de contractgegevens van de Onderwijsinstelling en de accounthouder, niet de gegevens van leerlingen.
- *Verbetering* is aangekruist uitsluitend in de betekenis die het Convenant eraan geeft — onderhoud, foutherstel, back-up en ondersteuning in opdracht van de Onderwijsinstelling. **De Verwerker gebruikt de Persoonsgegevens van Onderwijsdeelnemers niet om modellen te trainen, niet voor productonderzoek en niet voor statistiek over instellingen heen.**
- *Niet aangekruist* zijn onder meer adaptief leermateriaal, roosters, medische of begeleidingsgegevens, verstrekking aan derden en onderzoeksdoeleinden: het product biedt die functies niet.

F. Categorieën Persoonsgegevens inclusief bewaartermijnen

F.1 Betrokkenen en categorieën Persoonsgegevens

> **Lees dit eerst.** Zonder de optionele diensten onder D.2 verwerkt Puzzel.org **geen enkel** persoonsgegeven van een Onderwijsdeelnemer: een speler is anoniem en er wordt niets over hem of haar opgeslagen. Alles wat hieronder is aangekruist, is aangekruist omdat de docent het per activiteit kán aanzetten en het veld dan uit een vaste lijst kan kiezen — niet omdat het standaard wordt verwerkt.

Betrokkene: Onderwijsdeelnemer

Categorie persoonsgegevens	Specificatie	Aankruisen indien van toepassing op Verwerking(en)
Contactgegevens	Voorna(a)m(en)	☒ (optioneel, het registratieveld voornaam of naam; ook uit een klassenlijst of een SSO- of LTI-aanmelding)

Categorie persoonsgegevens	Specificatie	Aankruisen indien van toepassing op Verwerking(en)
	Voorletter(s)	☐
	Achternaam	☒ (optioneel, het registratieveld achternaam; ook uit een klassenlijst)
	Geslacht	☐
	Woonadres	☐
	Postcode	☐
	Woonplaats	☐
	Telefoonnummer	☒ (optioneel, het registratieveld telefoonnummer)
	E-mailadres (privé)	☒ (optioneel, het registratieveld e-mailadres; het formulier maakt geen onderscheid tussen privé en school)
	E-mailadres (school)	☒ (optioneel, het registratieveld e-mailadres; ook uit een klassenlijst, uit een Google-aanmelding of uit een start vanuit de leeromgeving)
Burgerservicenummer (BSN) of PGN		☐ — wordt niet gevraagd en niet verwerkt
Onderwijsdeelnemer-nummer	Een administratienummer dat Onderwijsdeelnemers identificeert	☒ (optioneel, het registratieveld leerlingnummer)
ECK-iD		☐ — niet ondersteund; er is geen Nummervoorziening- of KetenID-koppeling
Nationaliteit		☐
Geboortedatum		☐
Geboorteplaats		☐
Financiële gegevens met het oog op het berekenen, vastleggen en innen van gelden en bijdragen	Bankrekeningnummer	☐
	Facturenadministratie	☐
Gegevens over gezondheid*		☐ — wordt niet gevraagd. **Kanttekening:** de velden "overige informatie" en de zelf geformuleerde registratievraag zijn open velden. Als de Onderwijsinstelling daarin bijzondere persoonsgegevens laat invullen, gebeurt dat onder haar eigen verantwoordelijkheid en buiten deze bijsluiter om.
Godsdienst*		☐ — idem
Studievoortgang	Klas / leerjaar / ILT-code	☒ (optioneel, het registratieveld klas; ook als klasnaam in Puzzel LMS)
	Examinering	☐
	Studievoortgang en/of studietraject	☒ (de resultaten van een activiteit: voortgang, bestede tijd, score, aantal pogingen, en het behaalde cijfer bij een cijferkoppeling)

Categorie persoonsgegevens	Specificatie	Aankruisen indien van toepassing op Verwerking(en)
	Begeleiding Onderwijsdeelnemers, inclusief handelingsplan	☐
	Aan- en afwezigheidsregistratie	☐
Onderwijsorganisatie	Gegevens met het oog op de organisatie van het onderwijs (zoals een rooster) en het verstrekken of ter beschikking stellen van leermiddelen	☒ (welke activiteit of cursus aan de leerling is toegewezen, en het lidmaatschap van een klas in Puzzel LMS)
Beeldmateriaal	Foto's en videobeelden (beeldmateriaal) van Betrokkene met of zonder geluid van activiteiten van de Onderwijsinstelling	☒ — **niet door de leerling**: een leerling kan niets uploaden. Wél doordat de docent beeld- of geluidsmateriaal in een activiteit of cursus plaatst waarop leerlingen te zien of te horen zijn. Dat materiaal krijgt een publiek leesbare URL (zie D.1 onder 3).
Gebruikersgegevens	Diagnostische gegevens, loggegevens, metadata, anders namelijk …	☒ — tijdstip van aanmaken en laatst spelen, bestede tijd, voortgang, versienummer van de activiteit, en bij het activiteitstype "typen" de tekens die de leerling steeds miste; in Puzzel LMS een willekeurig apparaat-id met een grove apparaataanduiding en de tijdstippen waarop op dat apparaat een naam uit de klassenlijst werd gekozen of vrijgegeven (30 dagen bewaard)
	IP-adres	☒ — **met nadruk op de vorm.** Het IP-adres wordt niet als zodanig opgeslagen. Voor snelheidsbegrenzing wordt een met een geheim gezouten SHA-256-hash van het IP-adres bewaard. Het IP-adres zelf wordt wel verwerkt in het netwerkverkeer en in de logging van de hostingpartij (Vercel) en van de opslagpartijen; zie onderdeel G en H. Bij het inzenden van feedback of een melding over een bibliotheekitem wordt de user-agent van de melder in de e-mail aan de beheerder opgenomen.

Categorie persoonsgegevens	Specificatie	Aankruisen indien van toepassing op Verwerking(en)
Andere Persoonsgegevens, namelijk		☒ — • het tijdelijke, anonieme speler-id dat elke speler krijgt; • **de antwoorden en de vrije tekst die de leerling in een activiteit intypt** — dit is open invoer en kan alles bevatten wat de leerling schrijft; • een hash van een zelfgekozen wachtwoord, als de docent een wachtwoordveld of een klassenlijst met wachtwoorden gebruikt; • het account-id (en, afhankelijk van de instellingen, naam en e-mailadres) van een Google- of Microsoft-account waarmee de leerling zich aanmeldt; • het gebruikers-id dat de leeromgeving van de school bij een LTI-start meestuurt, en de naam en het e-mailadres voor zover de school die deelt; • het id van de inzending in Google Classroom en het laatst verzonden cijfer; • de organisatienaam, het land, het medewerkersnummer en de zelf geformuleerde vraag, voor zover de docent die velden aanzet; • **een eigen gebruikersaccount** bij Puzzel.org (voornaam, e-mailadres, taalvoorkeur) als de docent het registratieveld *wachtwoord* gebruikt — zie dienst 9; • in Puzzel LMS de score (0–100%) en de opmerking die de docent per activiteit bij het werk van de leerling vastlegt; • in Puzzel LMS het werk dat een leerling inlevert: de tekst die de leerling schrijft, de foto's en PDF's die de leerling toevoegt en de opmerking voor de docent — open invoer die alles kan bevatten wat de leerling schrijft of fotografeert, inclusief eerdere versies die bewaard blijven als de docent werk terugstuurt ter verbetering; de opmerking is vrije tekst van de docent; • bij meerspelervarianten: de opgegeven voornaam, het team, de beurtvolgorde en de ingezonden antwoorden in de spelsessie.

* Dit zijn bijzondere Persoonsgegevens die niet verwerkt mogen worden, tenzij is voldaan aan de eisen van de AVG en de UAVG.

Betrokkene: ouder/voogd/verzorger

Er worden geen Persoonsgegevens van ouders, voogden of verzorgers verwerkt. Het platform kent geen ouderrol, geen ouderaccount, geen oudercommunicatie en geen veld waarin oudergegevens worden gevraagd.

Categorie gegevens	Specificatie	Aankruisen indien van toepassing op Verwerking(en)
Contactgegevens	Voorna(a)m(en)	☐
	Voorletter(s)	☐
	Achternaam	☐
	Aanschrijftitel zoals geslacht	☐
	Woonadres	☐
	Postcode	☐
	Woonplaats	☐

Categorie gegevens	Specificatie	Aankruisen indien van toepassing op Verwerking(en)
	Telefoonnummer	☐
	E-mailadres (privé)	☐
Financiële gegevens met het oog op het berekenen, vastleggen en innen van gelden en bijdragen	Bankrekeningnummer	☐
	Facturenadministratie	☐
Gebruikersgegevens	Diagnostische gegevens, loggegevens, metadata, anders namelijk …	☐
	IP-adres	☐
Andere Persoonsgegevens, namelijk:		☐

Betrokkene: medewerker Onderwijsinstelling

Categorie gegevens	Specificatie	Aankruisen indien van toepassing op Verwerking(en)
Contactgegevens	Voorna(a)m(en)	☒ (verplicht bij het aanmaken van een account)
	Voorletter(s)	☐
	Achternaam	☒ (optioneel; wordt gevuld vanuit het profiel of bij SSO)
	Aanschrijftitel zoals geslacht	☐
	E-mailadres (school)	☒ (verplicht; is tevens de inlognaam)
Onderwijsorganisatie	Rooster	☐
	Begeleidingsgegevens	☐
Beeldmateriaal	Foto's en videobeelden (beeldmateriaal) van Betrokkene met of zonder geluid van activiteiten van de Onderwijsinstelling	☒ — voor zover de medewerker zulk materiaal zelf in een activiteit of cursus plaatst
Gebruiksgegevens	Diagnostische gegevens, zoals loggegevens, metadata, anders namelijk …	☒ — taalvoorkeur, abonnementsstatus en -datum, het aantal spelsessies deze maand, het aantal AI-tegoeden en de gestelde AI-vragen met de antwoorden, en de instellingen voor de opslagregio
	IP-adres	☒ — in dezelfde vorm en met dezelfde kanttekening als bij de Onderwijsdeelnemer hierboven

Categorie gegevens	Specificatie	Aankruisen indien van toepassing op Verwerking(en)
Andere Persoonsgegevens, namelijk:		☒ — • de inhoud die de medewerker maakt en uploadt (open velden: vragen, antwoorden, teksten, afbeeldingen, geluid, documenten); • de koppeling aan een schoolaccount; • factuurgegevens van de instelling en het klant-id bij Stripe, bij een betaald abonnement; • het Google-account-id, het e-mailadres en een versleuteld vernieuwingstoken bij een koppeling met Google Classroom; • een persoonlijke API-sleutel, als de medewerker de openbare API gebruikt; • de inhoud van e-mailcorrespondentie met de ondersteuning, in de mailbox van de Verwerker; • ingezonden feedback en ideeën voor de routekaart, met naam, e-mailadres, de bezochte pagina, de schermafmeting en de user-agent.

F.2 Bewaartermijn van de Persoonsgegevens of de criteria om die vast te stellen

De specifieke bewaartermijnen worden vastgesteld door de Onderwijsinstelling als Verwerkingsverantwoordelijke, eventueel op basis van een voorstel van de Verwerker. Hieronder staat wat het product feitelijk doet, en daarna het voorstel van de Verwerker.

Wat het product feitelijk doet:

Gegeven	Feitelijk gedrag
Activiteiten, resultaten, registraties, klassenlijsten, cursussen, feedback van de docent, ingeleverd werk	**Geen vaste bewaartermijn.** Deze gegevens blijven staan totdat de docent of de Onderwijsinstelling ze verwijdert. Er is geen automatische opschoning. De feedback bij een leerling en het werk dat die heeft ingeleverd (met eerdere versies en bestanden) gaan mee met het verwijderen van die leerling, van de klas, of met het resetten van de voortgang. De docent kan daarnaast elk los bestand verwijderen, of alle bestanden van leerlingen in een cursus tegelijk.
Het naamwissel-logboek van Puzzel LMS (apparaat-id, apparaataanduiding, tijdstippen)	**30 dagen.** Een dagelijkse taak verwijdert elke dag wat ouder is dan 30 dagen; het logboek van een klas verdwijnt ook met de klas.
Eén resultaat	Verwijderd zodra de docent het verwijdert.
Een activiteit	Bij verwijdering gaan de inhoud, de statistieken en de registraties van die activiteit mee.
Het account	Bij verwijdering worden alle gegevens die op het account-id staan in **beide** regio's verwijderd, worden de geüploade bestanden uit de bestandsopslag verwijderd, wordt het Google Classroom-token bij Google ingetrokken, en wordt de inlog bij Firebase Authentication verwijderd.
Reeds weggeschreven cijfers in Google Classroom of in de leeromgeving	Blijven daar staan: die horen bij het cijferregister van de school.
Meerspelerkamers van het type "challenge"	Worden door een dagelijkse taak verwijderd zodra ze **ouder dan 7 dagen** zijn.
Meerspelersessies van de overige typen en de bijbehorende registraties	**Worden door geen enkele taak opgeruimd.** Zij verdwijnen pas wanneer de docent de activiteit of de resultaten verwijdert, of bij verwijdering van het account.

Gegeven	Feitelijk gedrag
Deelnamecodes (join-PIN) en LTI-overdrachtsgegevens	Een LTI-overdracht is eenmalig bruikbaar en vervalt na 5 minuten (start van een activiteit) respectievelijk 30 minuten (deep link); een join-PIN vervalt op het door de docent gekozen moment. Beide worden daarnaast door een dagelijkse taak opgeruimd.
Uitnodigingen voor een schoolaccount	Vervallen na 30 dagen.
Snelheidsbegrenzing (gehashte IP-adressen)	Vervalt met het tijdvenster van de limiet; dagelijkse en maandelijkse tellers worden door de dagelijkse en maandelijkse taak gewist.
Bewaarde woordcontroles	Vervallen na het ingestelde tijdvenster.
De verzendregistratie van e-mail en de e-mailwachtrij	Blijven staan in de Amerikaanse database; deze gegevens worden **niet** door de accountverwijdering geraakt.
Betalings- en factuurgegevens	De betalingsadministratie en de bijbehorende boekhoudkundige gegevens staan buiten het account en worden **niet** door de accountverwijdering geraakt.
Ingezonden feedback en ideeën	Bevatten naam, e-mailadres, de bezochte pagina, de schermafmeting en de user-agent, en worden **niet** door de accountverwijdering geraakt.

Bewaartermijnen van de Verwerker. De applicatie dwingt geen automatische vervaltermijn af (behalve voor het naamwissel-logboek van Puzzel LMS, zie hierboven); de volgende termijnen gelden:

1. **Accounts, activiteiten, resultaten en registraties** blijven bewaard totdat de docent of de Onderwijsinstelling ze verwijdert. Dat kan op elk moment, in de applicatie zelf. Er is geen automatische verwijdering van inactieve accounts. De Onderwijsinstelling kan in onderdeel F.2 een eigen, kortere termijn opgeven en die zelf uitvoeren.
2. **Na beëindiging van de Verwerkersovereenkomst** (artikel 12 lid 2) — dat is: wanneer de Onderwijsinstelling stopt met het gebruik van Puzzel.org — worden de gegevens op schriftelijk verzoek binnen 30 dagen verwijderd, voor zover de Onderwijsinstelling dat niet al zelf heeft gedaan.
3. **Factuur- en betalingsgegevens** worden zeven jaar bewaard (fiscale bewaarplicht).
4. **De verzendregistratie van e-mail** wordt niet automatisch opgeschoond en wordt op verzoek verwijderd.
5. **Back-ups** van de database worden dagelijks door Firebase gemaakt en 30 dagen bewaard; verwijderde gegevens kunnen daarin dus nog maximaal 30 dagen aanwezig zijn (zie Bijlage 2).

G. Locatie van opslag en Verwerking Persoonsgegevens

> **Kernpunt, dat een Onderwijsinstelling expliciet moet wegen.** Puzzel.org kent twee onafhankelijke regio-instellingen per account: één voor de database en één voor de bestanden. Een nieuw account krijgt de regio die bij de tijdzone van de browser hoort: een browser in een Europese of Afrikaanse tijdzone krijgt **EU**. Een Nederlandse school die zich vanuit Nederland aanmeldt, komt dus in de EU-regio terecht. De **terugvalwaarde blijft echter de Verenigde Staten**, en accounts van vóór de invoering van de instelling staan in de Verenigde Staten. **Bovendien staat een aantal platformbrede gegevensverzamelingen altijd in de Verenigde Staten, ook voor een EU-account** (zie hieronder). De Onderwijsinstelling dient de regio-instelling van haar account(s) te controleren en zo nodig te laten wijzigen; wijzigen vereist een betaald abonnement en draait als achtergrondmigratie.

G.1 Plaats/land van opslag en Verwerking per Verwerking

Verwerking (zie onderdeel D)	Plaats/Land van opslag en Verwerking van de Persoonsgegevens
1, 2, 8, 9, 10, 11, 12, 16 — account, activiteiten, resultaten, registraties, klassen, schoolaccount (Google Firebase Realtime Database)	**België** als het account op de EU-regio staat; **Verenigde Staten** als het account op de VS-regio staat (standaard- en terugvalregio). De Amerikaanse instantie staat in Iowa. Volgens de documentatie van Firebase ligt de Europese instantie in België en de Amerikaanse in Iowa; de locatie van een instantie kan niet worden gewijzigd (firebase.google.com/docs/database/locations). Google vermeldt dat Verwerking door de dienst ook op andere Google Cloud-locaties kan plaatsvinden; de regio bepaalt waar de gegevens zijn opgeslagen.
1, 4, 11 — authenticatie (Google Firebase Authentication)	**Verenigde Staten, ongeacht de regio van het account.** Google vermeldt dat Firebase Authentication uitsluitend vanuit Amerikaanse datacenters draait en gegevens uitsluitend in de Verenigde Staten verwerkt (firebase.google.com/support/privacy). De regio is niet instelbaar. Dit betreft het e-mailadres en de inloggegevens van de docent, en het anonieme speler-id.
3 — geüploade afbeeldingen, geluid en documenten (Amazon S3)	**Zweden (Stockholm)** als het account op de EU-bestandsregio staat; **Verenigde Staten (Californië)** als het op de VS-regio staat. Een wijziging van de instelling geldt alleen voor nieuwe uploads; bestaande bestanden blijven staan waar ze staan.
3 — malwarecontrole van documenten (AWS GuardDuty Malware Protection for S3)	In de regio van de betreffende bestandsopslag. De malwarecontrole geldt uitsluitend voor documenten die in het cursusgedeelte (LMS) van Puzzel.org worden geüpload; afbeeldingen en geluid worden niet op malware gecontroleerd.
5, 6 en alle Verwerkingen — uitvoering van de applicatie en de API (Vercel)	**Frankfurt, Duitsland en Washington D.C., Verenigde Staten.** De functies draaien in beide regio's; Vercel stuurt elk verzoek naar de regio die het dichtst bij de bezoeker ligt, zodat een verzoek vanuit Nederland normaal gesproken in Frankfurt wordt verwerkt. Dit is een routeringsregel en geen harde garantie: bij een storing in Frankfurt kan een verzoek in de andere regio terechtkomen. Deze regiokeuze is op 19 september 2026 in de projectinstellingen van Vercel vastgelegd (Pro-abonnement) en is sinds de uitrol van diezelfde dag voor beide regio's actief.
Alle Verwerkingen — platformbrede gegevensverzamelingen	**Altijd de Verenigde Staten**, ook voor een EU-account. Met persoonsgegevens erin zijn dat onder meer: de e-mailwachtrij en de verzendregistratie van e-mail (met geadresseerde en naam), de index van uitnodigingen, de deelnamecodes, de registers en overdrachtsgegevens voor de koppeling met de leeromgeving (LTI), de betalingsadministratie, de snelheidsbegrenzers (met gehashte IP-adressen), en ingezonden feedback, ideeën en stemmen voor de routekaart.
6 — e-mail aan de accounthouder (Twilio SendGrid)	**Verenigde Staten.** De dienst wordt op het standaardeindpunt afgenomen; EU-dataresidentie bestaat bij Twilio SendGrid alleen als betaalde optie met een aparte EU-subgebruiker en is niet ingericht.
7 — weblettertypen	Wordt door de applicatie zelf geserveerd, vanaf dezelfde plaats als de applicatie (zie de rij Vercel hierboven). Er is geen derde partij bij betrokken en er is geen doorgifte.
13 — cijferkoppeling Google Classroom	Google, wereldwijd/Verenigde Staten, en het Google Workspace-domein van de school zelf.
14 — cijferkoppeling LTI 1.3	De leeromgeving van de school, op de plaats waar de school die host.
17, 18 — AI-assistent en woordcontrole (OpenAI)	**Verenigde Staten.** Er is geen regio, organisatie-eindpunt of nulretentie-optie ingesteld.
17 — AI-assistent voor beeld en documenten (Google Gemini)	Door Google beheerd, wereldwijd. Dit is de algemene Generative Language API, niet Vertex AI; er is geen regio in te stellen en er is er geen ingesteld.
17 — zoeken naar stockfoto's (Pixabay)	**Duitsland** (Pixabay GmbH). Alleen de zoekterm van de docent wordt verstuurd, vanaf de server; de browser van de gebruiker maakt geen verbinding met Pixabay.

Verwerking (zie onderdeel D)	Plaats/Land van opslag en Verwerking van de Persoonsgegevens
20 — betalingen (Stripe)	Ierland (contractspartij Stripe Payments Europe, Limited) met doorgifte naar Stripe, LLC in de **Verenigde Staten** en gelieerde ondernemingen wereldwijd; Stripe biedt geen verwerking uitsluitend binnen de EU.

G.2 Doorgifte buiten de EER

Bij meerdere Verwerkingen waarbij doorgifte naar een land buiten de EER plaatsvindt, is deze tabel meermaals gebruikt.

Doorgifte 1 — Google LLC / Google Cloud (Firebase Realtime Database in de VS-regio, Firebase Authentication, Gemini, Google Classroom)

Verwerking (zie onderdeel D)	1, 2, 4, 8–12, 13, 17
Beschrijving doorgifte buiten de EER	Opslag van accountgegevens, activiteiten en resultaten in de Amerikaanse database-instantie (voor accounts die niet op de EU-regio staan, en voor alle platformbrede gegevensverzamelingen); authenticatiegegevens; afbeeldingen en documenten die aan Gemini worden aangeboden; het cijfer en het account-id van een leerling bij een Google Classroom-koppeling.
Land van Verwerking of internationale organisatie	Verenigde Staten (Google LLC), en voor Gemini wereldwijd.
****Getroffen waarborgen* voor doorgifte****	De Firebase Data Processing and Security Terms maken deel uit van de overeenkomst met Google (firebase.google.com/terms/data-processing-terms) en hoeven niet afzonderlijk te worden ondertekend. Doorgifte berust op het EU-VS Data Privacy Framework, waaraan Google deelneemt, en op de Standard Contractual Clauses waar dat kader niet van toepassing is. Lijst van subverwerkers: firebase.google.com/terms/subprocessors. Voor de Gemini API gelden voor klanten in de EER de voorwaarden voor betaalde diensten: Google gebruikt prompts en antwoorden niet om zijn producten te verbeteren (ai.google.dev/gemini-api/terms); de Verwerking is niet aan een regio gebonden.
Onderwijsinstelling geeft Verwerker schriftelijke toestemming voor de hierboven opgenomen doorgiften aan derde landen of internationale organisaties	☐

Doorgifte 2 — Amazon Web Services (S3 in Californië, GuardDuty)

Verwerking (zie onderdeel D)	3
Beschrijving doorgifte buiten de EER	Opslag van door de docent geüploade afbeeldingen, geluidsfragmenten en documenten, voor accounts waarvan de bestandsregio op de Verenigde Staten staat. Die bestanden kunnen beeldmateriaal van leerlingen of medewerkers bevatten en zijn publiek leesbaar voor wie de URL heeft.
Land van Verwerking of internationale organisatie	Verenigde Staten (Californië). Voor accounts op de EU-bestandsregio blijft de opslag in Zweden (Stockholm) en is er geen doorgifte.
****Getroffen waarborgen* voor doorgifte****	Het AWS Data Processing Addendum maakt automatisch deel uit van de AWS Service Terms (artikel 1.14) en bevat de Standard Contractual Clauses (EU 2021/914); contractspartij is Amazon Web Services EMEA SARL (Luxemburg). AWS neemt daarnaast deel aan het EU-VS Data Privacy Framework. Tekst: d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.

Onderwijsinstelling geeft Verwerker schriftelijke toestemming voor de hierboven opgenomen doorgiften	□

Doorgifte 3 — Vercel Inc. (hosting en uitvoering van de applicatie)

Verwerking (zie onderdeel D)	Alle
Beschrijving doorgifte buiten de EER	Elke aanvraag aan de applicatie en elke API-aanroep passeert de servers van Vercel: registratiegegevens van leerlingen, gegeven antwoorden, resultaten, uploads en accountgegevens. Er wordt bij Vercel geen applicatiegegeven opgeslagen (er is geen Vercel-database of -objectopslag in gebruik), maar de gegevens worden er wel verwerkt en verschijnen in de logging van het platform.
Land van Verwerking of internationale organisatie	Duitsland (Frankfurt) en Verenigde Staten (Washington D.C.) — zie G.1. Contractspartij is Vercel Inc. (Verenigde Staten); Vercel heeft geen Europese entiteit.
Getroffen waarborgen* voor doorgifte	Het Vercel Data Processing Addendum is door verwijzing onderdeel van de voorwaarden en geldt voor Pro-klanten zonder ondertekening (vercel.com/legal/dpa). Het bevat de Standard Contractual Clauses van 2021; Vercel neemt daarnaast deel aan het EU-VS Data Privacy Framework. Subverwerkers: security.vercel.com.
Onderwijsinstelling geeft Verwerker schriftelijke toestemming voor de hierboven opgenomen doorgiften	□

Doorgifte 4 — OpenAI (AI-assistent en woordcontrole)

Verwerking (zie onderdeel D)	17, 18
Beschrijving doorgifte buiten de EER	Bij dienst 17: de vrije tekst die de docent invoert, en bij het vertalen van een activiteit de volledige tekst van die activiteit. Bij dienst 18: het losse woord dat een leerling bij het activiteitstype "wordle" intypt, zonder speler-id en zonder verdere context.
Land van Verwerking of internationale organisatie	Verenigde Staten.
Getroffen waarborgen* voor doorgifte	Het OpenAI Data Processing Addendum maakt deel uit van de overeenkomst (cdn.openai.com/pdf/openai-data-processing-addendum.pdf); contractspartij voor de EER is OpenAI Ireland Limited. Doorgifte berust op de Standard Contractual Clauses. Gegevens die via de API worden verzonden, worden niet gebruikt om modellen te trainen, tenzij de klant daarvoor kiest — dat is niet gedaan. OpenAI bewaart logboeken voor misbruikbewaking standaard maximaal 30 dagen. EU-dataresidentie en nulretentie vereisen een afzonderlijke afspraak met OpenAI en zijn niet ingericht. Subverwerkers: platform.openai.com/subprocessors.
Onderwijsinstelling geeft Verwerker schriftelijke toestemming voor de hierboven opgenomen doorgiften	□

Doorgifte 5 — Twilio SendGrid (e-mail aan accounthouders)

Verwerking (zie onderdeel D)	6
Beschrijving doorgifte buiten de EER	Naam en e-mailadres van de accounthouder en de inhoud van het bericht. Als de Onderwijsinstelling leerlingaccounts aanzet (dienst 12), ook de voornaam en het e-mailadres van de leerling en de e-mail om een wachtwoord te kiezen.

Land van Verwerking of internationale organisatie	Verenigde Staten.
****Getroffen waarborgen* voor doorgifte****	Het Twilio Data Protection Addendum "forms part of the agreement(s) between Customer and Twilio" (twilio.com/en-us/legal/data-protection-addendum) en bevat de Standard Contractual Clauses van 2021/914. Voor een klant die in de EER is gevestigd is de contractspartij Twilio Ireland Limited (Dublin), blijkens de entiteitentabel in de Twilio Terms of Service (twilio.com/en-us/legal/tos); Twilio Inc. in de Verenigde Staten is de importeur. Doorgifte berust op het EU-VS Data Privacy Framework, de Binding Corporate Rules van Twilio en de Standard Contractual Clauses. Subverwerkers: twilio.com/legal/sub-processors.
Onderwijsinstelling geeft Verwerker schriftelijke toestemming voor de hierboven opgenomen doorgiften	□

Doorgifte 6 — Stripe (betalingen)

Verwerking (zie onderdeel D)	20
Beschrijving doorgifte buiten de EER	E-mailadres en account-id van de accounthouder en de factuurgegevens van de instelling. Betreft geen gegevens van Onderwijsdeelnemers.
Land van Verwerking of internationale organisatie	Ierland (Stripe Payments Europe, Limited), met doorgifte naar Stripe, LLC in de Verenigde Staten.
****Getroffen waarborgen* voor doorgifte****	De Stripe Data Processing Agreement bepaalt zelf dat zij "onderworpen is aan en deel uitmaakt van de overeenkomst" (stripe.com/legal/dpa); het Data Transfers Addendum hoort daarbij (stripe.com/legal/dta). Voor een account buiten Noord- en Zuid-Amerika is de contractspartij Stripe Payments Europe, Limited (Ierland). Doorgifte berust op het EU-VS Data Privacy Framework en de Standard Contractual Clauses. Subverwerkers: stripe.com/legal/service-providers.
Onderwijsinstelling geeft Verwerker schriftelijke toestemming voor de hierboven opgenomen doorgiften	□

* Mogelijke waarborgen zijn bijvoorbeeld een adequaatheidsbesluit van de Europese Commissie voor het betreffende land of – bij het ontbreken daarvan, Standard Contractual Clauses (SCC), met, indien nodig, voldoende aanvullende maatregelen om de veiligheid van de doorgifte te waarborgen.

Let op, artikel 10 lid 1 van de Model Verwerkersovereenkomst. De Verwerker is uitsluitend gerechtigd tot doorgifte buiten de EER indien de Onderwijsinstelling daarvoor **specifieke schriftelijke toestemming** heeft gegeven. De aankruisvakjes in de tabellen hierboven zíjn die toestemming: een Onderwijsinstelling die deze bijlage ondertekent met een vakje aangekruist, geeft toestemming voor precies de daar beschreven doorgifte en voor geen andere.

Een Onderwijsinstelling die een bepaalde doorgifte liever niet toestaat, kan de tabellen lezen als een reeks keuzes, want de meeste doorgiften volgen uit een instelling of uit een optionele dienst:

- **Doorgifte 2 (geüploade bestanden) vervalt volledig** wanneer de bestandsregio van het account op de EU staat: de bestanden blijven dan in Stockholm.
- **Doorgifte 1 wordt kleiner** wanneer de databaseregio van het account op de EU staat. Wat ervan overblijft zijn de authenticatiegegevens — Firebase Authentication kent geen regio-instelling — samen met de platformbrede gegevensverzamelingen uit G.1, en de diensten 13 en 17 als de Onderwijsinstelling die aanzet.
- **Doorgifte 4 (OpenAI) ontstaat niet** als de Onderwijsinstelling de AI-assistent (dienst 17) niet gebruikt en het activiteitstype "wordle" (dienst 18) niet gebruikt. Beide staan uit tenzij een docent ernaar grijpt.

- **Doorgifte 6 (Stripe) ontstaat niet** zonder betaald abonnement, en betreft de contractgegevens van de Onderwijsinstelling, niet de gegevens van een leerling.
- **Doorgifte 5 (SendGrid)** betreft e-mail aan de accounthouder — een medewerker, en aan een leerling alleen als de Onderwijsinstelling leerlingaccounts aanzet (dienst 12): één e-mail om een wachtwoord te kiezen.
- **Doorgifte 3 (Vercel) is niet uit te zetten**, want het is de hosting waarop de applicatie draait. Een verzoek uit Nederland wordt normaal gesproken in Frankfurt verwerkt (zie G.1) en er worden bij Vercel geen applicatiegegevens opgeslagen.

Waar een doorgifte niet te vermijden is, gelden de waarborgen die in de tabellen hierboven zijn opgenomen. De Verwerker is bereid om over elk van deze punten een afwijking te bespreken; een overeengekomen afwijking wordt vastgelegd in Bijlage 3 (Wijzigingenbijlage).

H. Subverwerkers

Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van de volgende Subverwerkers:

Subverwerker 1

Naam Subverwerker	Google Ireland Limited / Google LLC — Firebase (Realtime Database en Authentication)
Soort Verwerking	Opslag van alle accountgegevens, activiteiten, resultaten, registraties, klassenlijsten en cursussen in twee database-instanties, en de authenticatie van docenten en spelers (inclusief de anonieme aanmelding van elke speler).
(Categorie) Persoonsgegevens die de Subverwerker verwerkt	Alle categorieën uit onderdeel F: contactgegevens, leerlingnummer, klas, studievoortgang en resultaten, gebruikersgegevens, gehashte wachtwoorden, e-mailadressen, en de door docenten en leerlingen ingevoerde vrije tekst.
Land van opslag/Verwerking Persoonsgegevens door Subverwerker	België voor accounts op de EU-regio; Verenigde Staten voor accounts op de VS-regio en voor alle platformbrede gegevensverzamelingen. Firebase Authentication: door Google beheerd, niet regionaal instelbaar.
Vestigingsland Subverwerker	Ierland (Google Ireland Limited) / Verenigde Staten (Google LLC). Zie onderdeel G, doorgifte 1.

Subverwerker 2

Naam Subverwerker	Amazon Web Services, Inc. / Amazon Web Services EMEA SARL — Amazon S3 en GuardDuty Malware Protection
Soort Verwerking	Opslag van door docenten geüploade afbeeldingen, geluidsfragmenten en documenten en van de foto's en PDF's die leerlingen in Puzzel LMS inleveren, en de malwarecontrole van geüploade documenten vóór publicatie.
(Categorie) Persoonsgegevens die de Subverwerker verwerkt	Beeld- en geluidsmateriaal en documenten die persoonsgegevens kunnen bevatten (waaronder beeldmateriaal van Onderwijsdeelnemers en medewerkers), met in de bestandssleutel het account-id van de docent.
Land van opslag/Verwerking Persoonsgegevens door Subverwerker	Zweden (Stockholm) voor accounts op de EU-bestandsregio; Verenigde Staten (Californië) voor accounts op de VS-bestandsregio.

Vestigingsland Subverwerker	Verenigde Staten / Luxemburg. Zie onderdeel G, doorgifte 2.

Subverwerker 3

Naam Subverwerker	Vercel Inc.
Soort Verwerking	Hosting, levering en uitvoering van de webapplicatie en van alle API-eindpunten, inclusief de geplande taken. Alle gegevensverkeer tussen de browser en de opslag passeert deze partij.
(Categorie) Persoonsgegevens die de Subverwerker verwerkt	Alle categorieën uit onderdeel F, in doorvoer; daarnaast verbindingsgegevens waaronder het IP-adres van de bezoeker. Er wordt bij deze Subverwerker geen applicatiegegeven opgeslagen.
Land van opslag/Verwerking Persoonsgegevens door Subverwerker	Duitsland (Frankfurt) en Verenigde Staten (Washington D.C.); een verzoek gaat naar de dichtstbijzijnde regio. Zie onderdeel G.
Vestigingsland Subverwerker	Verenigde Staten. Zie onderdeel G, doorgifte 3.

Subverwerker 4

Naam Subverwerker	OpenAI Ireland Limited (contractspartij voor klanten in de EER); de Verwerking vindt plaats bij OpenAI, L.L.C. in de Verenigde Staten
Soort Verwerking	Het genereren van inhoud op verzoek van een docent (dienst 17) en het controleren of een door een leerling ingetypt woord bestaat (dienst 18).
(Categorie) Persoonsgegevens die de Subverwerker verwerkt	Bij dienst 17: de vrije tekst die de docent invoert, inclusief de volledige tekst van een activiteit bij een vertaalopdracht — die tekst kan persoonsgegevens bevatten als de docent die erin heeft gezet. Bij dienst 18: één door een leerling ingetypt woord, zonder identificerende gegevens.
Land van opslag/Verwerking Persoonsgegevens door Subverwerker	Verenigde Staten.
Vestigingsland Subverwerker	Verenigde Staten. Zie onderdeel G, doorgifte 4.

Subverwerker 5

Naam Subverwerker	Google Ireland Limited / Google LLC — Gemini (Generative Language API)
Soort Verwerking	Het omzetten van een geüpload document, werkblad of foto in opgaven, en het genereren en bewerken van afbeeldingen, op verzoek van een docent (dienst 17).
(Categorie) Persoonsgegevens die de Subverwerker verwerkt	De volledige inhoud van het door de docent geüploade bestand of de geüploade afbeelding, inclusief eventuele persoonsgegevens daarin, en de ingevoerde omschrijving.
Land van opslag/Verwerking Persoonsgegevens door Subverwerker	Wereldwijd; er is geen regio instelbaar op de gebruikte API.
Vestigingsland Subverwerker	Ierland / Verenigde Staten. Zie onderdeel G, doorgifte 1.

Subverwerker 6

Naam Subverwerker	Twilio Inc. — SendGrid
Soort Verwerking	Het verzenden van e-mail aan de accounthouder over het account, het abonnement, uitnodigingen, limieten en platformberichten; en, alleen als de Onderwijsinstelling leerlingaccounts aanzet (dienst 12), de e-mail waarmee een Onderwijsdeelnemer een wachtwoord kiest of opnieuw instelt.
(Categorie) Persoonsgegevens die de Subverwerker verwerkt	Naam en e-mailadres van de medewerker van de Onderwijsinstelling, en de inhoud van het bericht; met leerlingaccounts ook de voornaam en het e-mailadres van de Onderwijsdeelnemer.
Land van opslag/Verwerking Persoonsgegevens door Subverwerker	Verenigde Staten.
Vestigingsland Subverwerker	Verenigde Staten. Zie onderdeel G, doorgifte 5.

Subverwerker 7

Naam Subverwerker	Stripe Payments Europe, Limited (contractspartij); doorgifte naar Stripe, LLC
Soort Verwerking	Het afhandelen van betalingen, abonnementen en facturatie voor een betaald abonnement. Betaalkaartgegevens worden uitsluitend bij Stripe ingevoerd en verwerkt.
(Categorie) Persoonsgegevens die de Subverwerker verwerkt	E-mailadres en account-id van de accounthouder, factuurgegevens van de instelling, en de betaalgegevens die de betaler bij Stripe invoert. Geen gegevens van Onderwijsdeelnemers.
Land van opslag/Verwerking Persoonsgegevens door Subverwerker	Ierland en Verenigde Staten
Vestigingsland Subverwerker	Ierland. Zie onderdeel G, doorgifte 6.

Subverwerker 8

Naam Subverwerker	Pixabay GmbH
Soort Verwerking	Het doorzoeken van een stockfotobibliotheek op verzoek van een docent. De zoekopdracht wordt vanaf de server verstuurd; de browser van de gebruiker maakt geen verbinding met Pixabay, en een gekozen foto wordt naar de eigen opslag gekopieerd.
(Categorie) Persoonsgegevens die de Subverwerker verwerkt	Uitsluitend de zoekterm die de docent intypt. Er wordt geen account-id, IP-adres of ander identificerend gegeven meegestuurd.
Land van opslag/Verwerking Persoonsgegevens door Subverwerker	Duitsland.
Vestigingsland Subverwerker	Duitsland.

Overige ontvangers — geen Subverwerkers

De volgende partijen ontvangen persoonsgegevens, maar niet als Subverwerker van Puzzel.org. Zij worden hier vermeld omdat de Onderwijsinstelling ze moet kunnen wegen.

Partij	Rol en ontvangen gegevens
Google Classroom, binnen het Workspace-domein van de school	De school is zelf verwerkingsverantwoordelijke voor haar Classroom-omgeving. Puzzel.org zendt daar op instructie van de docent uitsluitend het behaalde cijfer naartoe, naar een inzending die al in de klas van die docent bestaat.
De leeromgeving van de school (LTI 1.3)	Idem: de school host en beheert het platform zelf; Puzzel.org zendt er uitsluitend het behaalde cijfer naartoe en ontvangt de identiteitsgegevens die de school zelf deelt.
Door de docent ingesloten video en documenten	Plaatst een docent een YouTube- of Vimeo-video of een Google Drive- of OneDrive-document in een cursus, dan maakt de browser van de leerling verbinding met die partij. Er worden uitsluitend privacyvriendelijke varianten toegestaan (YouTube in de cookievrije modus, Vimeo met het volgen uitgeschakeld); willekeurige insluitingen worden geweigerd.

Verwerker heeft — na het afsluiten van de Verwerkersovereenkomst — het recht gebruik te maken van andere dan de in deze Privacybijsluiter vermelde Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Onderwijsinstelling, en Onderwijsinstelling daartegen binnen zes weken bezwaar kan maken (artikel 11 lid 2 Model Verwerkersovereenkomst).

Bijlage 1 (Privacybijsluiter) maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad, de verschillende betrokken ketenpartijen (MEVW, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u op www.privacyconvenant.nl.

MODEL BIJLAGE 2: BEVEILIGINGSBIJLAGE Puzzel.org

Verwerker: **Puzzel.org**. Versie **1.2**, datum laatste aanpassing **25 september 2026**.

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 van de Model Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

Een deel van de maatregelen die het model als vanzelfsprekend opsomt, gaat uit van een organisatie met meerdere medewerkers en een ingericht beheerproces. Puzzel.org is een eenmansbedrijf. Waar een maatregel feitelijk niet bestaat, staat dat in deze bijlage als "Niet voldaan", met de reden erbij, in plaats van een geruststellende formulering. De Verwerker beschouwt een eerlijke beveiligingsbijlage met openstaande punten als een kleiner risico voor de Onderwijsinstelling dan een vleiende.

A. Maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking

1. Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast.

Het beleid is vastgelegd in een kort document, *Informatiebeveiligingsbeleid Puzzel.org*, vastgesteld op **20 september 2026**. Het wordt jaarlijks geëvalueerd, tegelijk met de self-assessment onder onderdeel B en na elk incident van betekenis.

Wat er feitelijk wél is, en wat als grondslag voor dat beleid kan dienen:

- De toegang tot gegevens wordt afgedwongen door de toegangsregels van de database, die op de servers van Google worden toegepast en niet in de browser. De database is standaard gesloten: er is geen algemene lees- of schrijfrecht op het hoogste niveau, waardoor elk gegevensonderdeel dat niet uitdrukkelijk is opengezet, dicht staat.
- In september 2026 zijn twee onafhankelijke beveiligingsonderzoeken uitgevoerd (zie onderdeel B, "Toetsvorm") en zijn de bevindingen daaruit grotendeels verwerkt.
- Wijzigingen aan de toegangsregels worden bijgehouden in een wijzigingenlogboek bij die regels zelf.

2. Verwerker neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

- **Puzzel.org heeft één medewerker**, tevens eigenaar. Er is geen tweede persoon aan wie rechten zijn toegekend, en dus ook geen functiescheiding. Dit is de feitelijke situatie. Komt er ooit een tweede persoon bij, dan krijgt die uitsluitend de rechten die voor de taak nodig zijn, en wordt deze bijlage daarop aangepast.
- **Voor de gebruiker is de autorisatie wél systematisch.** Elke lees- en schrijfbewerking gaat langs de toegangsregels van de database. Een account bereikt uitsluitend de eigen gegevens en de resultaten die op de eigen activiteiten zijn ingezonden. Een Onderwijsdeelnemer kan uitsluitend het eigen resultaat lezen: de regels toetsen daarvoor of het ingelogde account de speler zelf is. Een docent die aan een schoolaccount is verbonden, krijgt toegang tot de gedeelde bibliotheek van die school, en alleen langs een voorwaarde die aan de identificatie van die school is gekoppeld.
- **Beheerderstoegang** (de "puzzle master"-console, 52 eindpunten) vereist een door de server geverifieerd inlogtoken én een beheerdersrecord in de database. Dat record is uitsluitend door servercode te schrijven en voor iedere gebruiker onbeschrijfbaar, zodat niemand zichzelf beheerder kan maken.

- **Toegang tot een klantaccount voor ondersteuning.** Er is een functie waarmee de beheerder als een gebruiker kan inloggen. Die functie is beveiligd met dezelfde beheerderscontrole en kent **geen tweede factor en geen reden-veld**. Elk gebruik wordt wél vastgelegd: welke beheerder, welk account en wanneer, met interne accountnummers en zonder e-mailadres. Die vastlegging gebeurt vóórdat de toegang wordt verleend; lukt zij niet, dan wordt de toegang geweigerd. Dat de functie alleen op uitdrukkelijk verzoek van de accounthouder wordt gebruikt, en alleen om een gemeld probleem te onderzoeken, is een werkafspraak en geen technische maatregel; de gepubliceerde leveranciersinformatie stelt hetzelfde.

3. Verwerker heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van Persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.

Deze rol wordt vervuld door de eigenaar, die tevens de enige medewerker is. Er is geen onafhankelijke coördinator. Dit is de feitelijke situatie. Er is geen onafhankelijke controle binnen de organisatie; de onderzoeken onder onderdeel B zijn het middel waarmee de eigen beoordeling wordt getoetst.

4. Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.

Er wordt een incidentenregister bijgehouden: per incident de datum van ontdekking, de aard, de getroffen gegevens en Betrokkenen, de genomen maatregelen en de datum van afsluiting.

5. Verwerker heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Zie onderdeel C. Melding gebeurt per e-mail aan de accounthouder, door de contactpersoon in onderdeel C. De Onderwijsinstelling wordt onverwijld geïnformeerd, en uiterlijk binnen 48 uur na ontdekking.

6. Verwerker sluit met medewerkers geheimhoudingsverklaringen af en maakt informatiebeveiligingsafspraken.

Niet van toepassing: er zijn geen medewerkers naast de eigenaar. De geheimhoudingsplicht van de eigenaar vloeit voort uit artikel 6 van de Model Verwerkersovereenkomst zelf. Een eventuele toekomstige medewerker of ingehuurde kracht tekent vooraf een geheimhoudingsverklaring.

7. Verwerker stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.

Er is geen formeel opleidingsprogramma; de organisatie bestaat uit één persoon. De eigenaar voert jaarlijks de self-assessment onder onderdeel B uit, volgt de beveiligingsadviezen voor de gebruikte softwareafhankelijkheden op en laat de software periodiek op beveiliging onderzoeken.

B. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen

Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden. Verwerker gebruikt hiervoor in beginsel het 'Certificeringsschema informatiebeveiliging en privacy ROSA' (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy.

Toetsvorm	**Self-assessment (niveau 1).** De verklaring wordt door de eigenaar zelf afgegeven. Doorlopen op **20 september 2026** en bijgewerkt op **25 september 2026**, op basis van het Certificeringsschema toetsingskader **v4.0** (Edustandaard, december 2025).
Uitvoerder toets	Puzzel.org — Daan Weustenraad, eigenaar
Inlogpagina	https://puzzel.org/nl/auth

BIV-classificatie	**Beschikbaarheid = M**, **Integriteit = M**, **Vertrouwelijkheid = M**, vastgesteld volgens de classificatievragen van het Certificeringsschema toetsingskader v4.0 (Edustandaard, december 2025), waarin per aspect het hoogste antwoord telt. _Onderbouwing:_ het product is oefen- en toetsmateriaal, geen leerlingadministratie- of leerlingvolgsysteem en geen examensysteem; uitval raakt geen wettelijke registratie, maar de dienst wordt ook 's avonds en in het weekend gebruikt, een storing van dagen is niet aanvaardbaar, en uitval belemmert een les die wel kan doorgaan (B = midden). De resultaten worden door docenten gebruikt om voortgang te beoordelen en kunnen als cijfer naar een cijferregister worden geschreven, waardoor onjuistheid gevolgen heeft (I = midden). Er worden geen bijzondere persoonsgegevens en geen BSN verwerkt, maar wel namen, e-mailadressen, leerlingnummers en leerresultaten van minderjarigen (V = midden). **Een school die het product voor toetsing met gevolgen inzet, moet zelf beoordelen of I en V voor haar hoger uitvallen.**

Categorie	Maatregelen	Compliance	Uitleg
Beschikbaarheid	Ontwerp	Voldaan	De redundantie wordt geleverd door Vercel en Google, en een externe beschikbaarheidscontrole geeft kennisgeving van uitval (zie de rij "Monitoring"). De applicatie draait serverloos bij Vercel en de gegevens staan in Google Firebase Realtime Database; beide zijn beheerde, redundant uitgevoerde diensten. Er is geen eigen server- of netwerkapparatuur. De spelpagina leest de inhoud rechtstreeks uit de database en is daarmee niet afhankelijk van de beschikbaarheid van de eigen serverfuncties.
	Capaciteit beheer	Niet voldaan	**Afwijking (niveau Midden):** er is geen trendanalyse en geen actieve signalering op een vooraf gestelde norm; schaling is geheel aan Vercel en Google overgelaten. Schaling wordt door Vercel en Google beheerd. Op applicatieniveau zijn er snelheidsbegrenzers op circa 25 publieke eindpunten en een limiet van 10 aanroepen per dag per sleutel op de openbare API.
	Onderhoud	Niet voldaan	**Afwijking (niveau Midden):** onderhoud vindt niet gepland plaats, en één softwareafhankelijkheid is bewust nog niet bijgewerkt terwijl er een beveiligingsadvies voor openstaat. Een rollback-scenario is er wel: Vercel kan elke eerdere uitrol direct terugzetten. Onderhoud wordt door de eigenaar uitgevoerd; er is geen onderhoudsvenster en geen afgesproken servicewindow. Er wordt geen beschikbaarheidsafspraak of SLA aangeboden: de dienst wordt naar beste vermogen geleverd, met ondersteuning per e-mail tussen 09:00 en 22:00 CET.
	Testen	Niet voldaan	**Afwijking (niveau Midden):** er is geen regressietest op beschikbaarheid na een release, geen jaarlijkse loadtest en geen geautomatiseerde bouwstraat; tests en typecontrole worden met de hand gestart. Er is een geautomatiseerde typecontrole over de gehele software en er zijn eenheidstests, waaronder een testreeks tegen de toegangsregels van de database op een lokale emulator. Er is **geen** acceptatieomgeving met echte gegevens; wijzigingen worden op een voorvertoning van Vercel en lokaal beproefd.
	Monitoring	Voldaan	Een externe beschikbaarheidscontrole (UptimeRobot) controleert elke vijf minuten de website en een serverroute, telkens op de inhoud van het antwoord en niet alleen op de statuscode, en waarschuwt de eigenaar per e-mail bij uitval. De dienst bewaart drie maanden beschikbaarheidsgeschiedenis, die een Onderwijsinstelling op verzoek kan krijgen. Er is geen aparte foutmonitoringdienst: fouten in de applicatie zelf worden opgemerkt door de eigenaar of door een melding van een gebruiker.

Categorie	Maatregelen	Compliance	Uitleg
	Herstel	Niet voldaan	**Afwijking (niveau Midden):** de norm eist een periodieke hersteltest; die vindt niet plaats. Dit is een bewust aanvaard risico. Herstel van de database is mogelijk uit de dagelijkse back-up van Firebase (zie de rij "Back-up"). Het herstelproces is niet beproefd, en voor geüploade bestanden is er geen herstelmogelijkheid.
Integriteit	Herleidbaarheid (gebruikers)	Niet voldaan	**Afwijking:** wijzigingen kunnen niet per stuk worden teruggedraaid (er is geen versiehistorie, alleen de dagelijkse back-up) en wijzigingen van gegevens zijn niet achteraf inzichtelijk. De tijdstempels op een resultaat worden door de browser van de speler gezet, niet door de server. Elke schrijfbewerking is aan een geverifieerde gebruiker gebonden: de toegangsregels toetsen welk account is ingelogd, en elke serveraanroep verifieert het inlogtoken. Bij een resultaat wordt gecontroleerd dat het onder de eigen speler wordt weggeschreven, zodat een speler geen rij onder de naam van een ander kan wegschrijven. Cijfers worden op de server berekend uit de gegeven antwoorden en nooit uit de browser overgenomen.
	Back-up	Niet voldaan	**Afwijking:** de dagelijkse frequentie wordt gehaald, maar de integriteit van de back-up wordt niet per kwartaal gecontroleerd, er is geen functiescheiding (één persoon) en geüploade bestanden hebben geen back-up (bewust aanvaard risico, zie hierna). Voor beide instanties van de Firebase Realtime Database (VS en EU) zijn de **dagelijkse automatische back-ups** van Firebase ingeschakeld; een back-up wordt 30 dagen bewaard. Voor de geüploade bestanden in Amazon S3 is **geen versiebeheer en geen back-up** ingericht: een verwijderd of overschreven bestand kan niet worden teruggehaald. Dit is een bewust aanvaard risico: het gaat om afbeeldingen, geluid en documenten bij activiteiten, die de docent opnieuw kan uploaden, en om foto's en PDF's die leerlingen in Puzzel LMS inleveren, waarvan de leerling het origineel normaal gesproken zelf heeft; resultaten en registraties van leerlingen staan in de database en vallen wél onder de dagelijkse back-up. Amazon S3 bewaart elk bestand zelf redundant op meerdere locaties, zodat uitval van apparatuur niet tot verlies leidt. Er is geen beproefde herstelprocedure.
	Application controls	Alternatieve maatregel	**Alternatieve maatregel:** de speelgegevens gaan bewust rechtstreeks van de browser naar de database, zodat wijzigingen niet langs een eigen applicatielaag lopen; de toegangsregels van de database, die op de servers van Google worden toegepast, vervullen die controlerende rol. Invoer wordt zowel in die regels als op de server gevalideerd: lengtebegrenzingen en toegestane velden op ingezonden gegevens (bijvoorbeeld een ranglijstrij met zeven toegestane velden en een label van maximaal 500 tekens), een strikt patroon op de woordcontrole, en typedetectie op geüploade bestanden op basis van de inhoud van het bestand in plaats van wat de browser meldt. Uitgaande HTML in e-mail wordt geschoond.
	Onweerlegbaarheid (gegevens)	Niet voldaan	**Afwijking:** de norm vraagt functionele logging van wijzigingen van (persoons)gegevens, 13 maanden bewaard. Zo'n wijzigingslog bestaat niet. Bij een resultaat wordt wel vastgelegd wie de speler is, van wie de activiteit is, wanneer het is aangemaakt en wanneer het voor het laatst is gespeeld. Een gewijzigd cijfer in het cijferregister is bij de school zichtbaar.

Categorie	Maatregelen	Compliance	Uitleg
	Herleidbaarheid (technisch beheer)	Niet voldaan	Alle wijzigingen aan de software staan in een versiebeheersysteem met auteur en tijdstip. Wijzigingen aan de toegangsregels van de database worden **met de hand** in de twee beheerconsoles van Google geplakt; er is één vastgelegde referentieversie van die regels, maar die is niet de bron van waarheid. Dit is een bewust geaccepteerd risico op afwijking tussen de twee regio's; na elke wijziging worden de regels in beide consoles naast de referentieversie gelegd. Beheerderstoegang tot een klantaccount wordt vastgelegd (zie A.2).
	Controle integriteit	Niet voldaan	**Afwijking:** de malwarecontrole geldt alleen voor documenten in het cursusgedeelte; afbeeldingen en geluid worden niet gecontroleerd. Er is geen vastgelegde richtlijn voor veilig programmeren en geen structurele controle van de configuratie. Geüploade documenten worden in quarantaine op malware gecontroleerd voordat zij publiceerbaar worden, en gepubliceerd via een kopie binnen de opslagdienst, zodat het gepubliceerde bestand exact het gecontroleerde bestand is. Bestandstypen worden uit de inhoud van het bestand afgeleid.
	Onweerlegbaarheid (applicatie)	Niet voldaan	**Afwijking:** de norm vraagt technische logging van beheerdersactiviteit en van aanpassingen aan configuratie en toepassing, met maandelijkse controle. Elke keer dat de eigenaar als een accounthouder inlogt wordt vastgelegd (wie, welk account, wanneer); overige beheerhandelingen en configuratiewijzigingen worden niet gelogd, en er is geen maandelijkse controle. Berichten aan de leeromgeving van een school worden ondertekend met een sleutel die alleen in de draaiende omgeving bestaat en waarvan de publieke helft op een vast adres wordt gepubliceerd; binnenkomende berichten worden tegen de publieke sleutels van het platform van de school gecontroleerd. De statuswaarde die bij het koppelen aan een cijferregister wordt meegegeven, is ondertekend en maximaal 30 minuten geldig.
Vertrouwelijkheid	Levenscyclus gegevens	Niet voldaan	**Afwijking:** er is geen automatische bewaartermijn; gegevens blijven staan totdat de docent of de Onderwijsinstelling ze verwijdert. Zie onderdeel F.2 van Bijlage 1. Verwijdering van een account wist alle aan het account gekoppelde gegevens in **beide** regio's, verwijdert de bestanden uit de objectopslag, trekt het Google Classroom-token bij Google in en verwijdert de inlog. **Niet gewist worden** enkele platformbrede gegevens (verzendregistratie van e-mail, betalingsadministratie, ingezonden feedback). Er is **geen** automatische vervaltermijn voor resultaten en registraties.
	Logische toegang	Niet voldaan	**Afwijking:** de norm eist tweefactorauthenticatie, standaard afgedwongen voor iedere gebruiker die gegevens van anderen ziet, en wachtwoordeisen volgens NIST. De applicatie biedt geen eigen tweefactorauthenticatie; een docent die met Google of Microsoft inlogt, neemt die van de aanbieder over, een docent met e-mailadres en wachtwoord niet. Het minimum voor een wachtwoord is acht tekens, afgedwongen door Firebase Authentication; de aanmeldpagina en het wachtwoordwijzigingsscherm noemen datzelfde minimum. De toegang zelf wordt afgedwongen door de toegangsregels op de servers van Google; zie A.2. Eén bijzonderheid moet hier worden genoemd: de oplossingen van een activiteit staan in een apart deel van de database dat alleen voor de eigenaar leesbaar is, omdat de spelpagina de inhoud rechtstreeks uit de database leest. De omzetting gebeurt bij het (opnieuw) opslaan van een activiteit; **oudere, niet opnieuw opgeslagen activiteiten dragen hun oplossingen nog in het publiek leesbare inhoudsdeel.**

Categorie	Maatregelen	Compliance	Uitleg
	Fysieke toegang	Voldaan	Er is geen eigen datacenter en geen eigen apparatuur. Fysieke beveiliging berust bij Google, Amazon Web Services en Vercel; zie onderdeel H van Bijlage 1.
	Netwerktoegang	Alternatieve maatregel	**Alternatieve maatregel:** er is geen eigen netwerk en dus geen netwerkzones of jump server. Beheer verloopt uitsluitend via de beheerconsoles van Google, Amazon Web Services en Vercel, die alle drie met tweefactorauthenticatie zijn beveiligd. Al het verkeer verloopt over HTTPS. Er is geen eigen netwerk en geen VPN. De verbinding met de database loopt over een versleutelde verbinding. Toegang tot de beheeromgeving vereist hetzelfde geverifieerde token als hierboven.
	Scheiding omgevingen	Niet voldaan	Er is geen aparte acceptatie- of testdatabase: beide databases zijn productie en er bestaat geen staging-kopie. Er geldt een vast werkvoorschrift dat er geen testgegevens naar de productiedatabases worden geschreven; voor controles van begin tot eind is één testaccount aangewezen. Wijzigingen worden lokaal en op een voorvertoning van Vercel beproefd.
	Transport en fysieke opslag	Voldaan	**Gemeten.** De conformiteit met de Uniforme Beveiligingsvoorschriften TLS van Edustandaard is op 20 september 2026 gemeten met internet.nl; het onderdeel HTTPS ("Verbinding voldoende beveiligd") is volledig groen, evenals DNSSEC en RPKI. Versleuteld transport (HTTPS/TLS) naar alle diensten, met HSTS voor een jaar inclusief subdomeinen en opname in de voorlaadlijst van de browsers, en met afdwingen van een versleutelde verbinding. Er vindt geen fysiek transport of fysieke opslag van gegevensdragers plaats.
	Logging	Niet voldaan	**Afwijking:** de norm eist logging van geslaagde en mislukte toegang en van het lezen van persoonsgegevens; geen van beide bestaat. Er wordt in de applicatie **geen** verzoeklogboek bijgehouden; er is geen logregel die een IP-adres of een e-mailadres wegschrijft. De weinige serverregels die een persoon kunnen raken, noemen een intern accountnummer of een gehashte waarde. Onderliggende logging van de hostingpartij valt buiten de applicatie. De keerzijde is dat er geen toegangslogboek is om een incident mee te reconstrueren; bij een incident is alleen de standaardlogging van Vercel beschikbaar, die kort wordt bewaard. Bij de gekozen classificatie (V = midden) is dit een erkende afwijking.
	Omgaan met kwetsbaarheden	Niet voldaan	**Afwijking:** drie bevindingen uit het onderzoek van 13 september 2026 staan nog open: activiteiten met een toegangsbeperking zijn buiten de browser om leesbaar; het decoderen van zeer grote afbeeldingen is nog niet begrensd (het overige deel van die bevinding is wel gesloten); en één softwareafhankelijkheid is bewust nog niet bijgewerkt terwijl er een beveiligingsadvies voor openstaat. De conformiteit met de Uniforme Beveiligingsvoorschriften TLS van Edustandaard, waarnaar deze norm verwijst, is op 20 september 2026 gemeten en in orde bevonden (zie de rij "Transport en fysieke opslag"). Softwareafhankelijkheden worden bijgehouden en beveiligingsmeldingen worden opgevolgd; een aantal onderdelen is bewust op een vaste versie gezet omdat een nieuwere versie in productie faalt, en de redenen daarvoor zijn vastgelegd. In september 2026 zijn twee onafhankelijke onderzoeken uitgevoerd (zie hieronder), waarvan de bevindingen grotendeels zijn verwerkt. Kwetsbaarheden worden naar ernst opgelost: **kritiek binnen 2 dagen, hoog binnen 30 dagen** na vaststelling. Kwetsbaarheden kunnen worden gemeld via daan@puzzel.org.

Uitgevoerde onderzoeken

Twee onderzoeken zijn in september 2026 uitgevoerd en schriftelijk vastgelegd. Beide zijn **onderzoeken van de software en de configuratie, ondersteund door tests op een lokale database-emulator — geen penetratietest van de draaiende dienst.**

1. **Beveiligingsonderzoek van 13 september 2026.** Omvang: 139 eindpunten waarvan 49 beheerderseindpunten, de gedeelde authenticatie, de toegangsregels van de database, de facturatie en webhooks, de opslag, de spelerregistratie en resultaten, de rechten rond schoolaccounts en de bibliotheek, en een zoektocht naar geheimen in de software. Dertien bevindingen: één kritiek (mits de sleutel actief bleef), zeven hoog, vijf midden.
2. **Onderzoek naar het verschil tussen de software en de toegangsregels, van 13 september 2026.** Ongeveer 35 bevindingen op de naad tussen wat de software doet en wat de toegangsregels toestaan, elk door een tweede beoordelaar getoetst en op de emulator nagerekend.

Stand van zaken. Van de dertien bevindingen uit het beveiligingsonderzoek zijn er tien afgesloten, waaronder de kritieke bevinding (een sleutel voor servertoegang, ingetrokken en geverifieerd) en de bevinding uit het tweede onderzoek over meerspelersessies; de bijbehorende regels staan in beide beheerconsoles. **Drie bevindingen staan open.**

- Activiteiten met een toegangsbeperking zijn buiten de browser om leesbaar. Deze bevinding is nog niet opgelost; er ligt een uitgewerkt plan.
- De bevinding over de belasting van de server door uploads is grotendeels gesloten: het uploaden van afbeeldingen en de meting bij zoek-de-verschillen kennen een limiet per gebruiker en per adres. Open blijft dat een zeer grote afbeelding volledig wordt gedecodeerd voordat de afmetingen bekend zijn.
- Eén softwareafhankelijkheid is nog niet bijgewerkt naar de versie waarin het openstaande beveiligingsadvies is verholpen.

De regels in beide beheerconsoles zijn gelijk aan de vastgelegde referentieversie.

Maatregelen die op applicatieniveau zijn getroffen

- Een gesloten database als uitgangspunt; geen enkel publiek beschrijfbaar pad. Het hoogste niveau van de toegangsregels kent zelf geen lees- of schrijfrecht en geen jokerteken, zodat elk gegevensonderdeel zonder eigen regel gesloten is. Negen in gebruik zijnde gegevensonderdelen hebben daardoor **geen eigen regel** — onder meer de vastlegging van beheerderstoegang, de betalingsadministratie en de verwerking van betalingsmeldingen. Alle negen worden uitsluitend door servercode gelezen en geschreven, met beheerdersrechten die de regels sowieso omzeilen; voor de browser zijn zij dicht.
- Resultaten per speler afgeschermd: een speler leest alleen de eigen rij.
- Oplossingen van activiteiten in een apart deel van de database dat alleen voor de eigenaar leesbaar is.
- De ranglijst als afgeschermde weergave met gemaskeerde e-mailadressen en telefoonnummers.
- Beheerderseindpunten uitsluitend op een geverifieerd inlogtoken plus een door de server geschreven beheerdersrecord.
- Beveiligingskoppen op elke respons: HSTS (1 jaar, inclusief subdomeinen, met opname in de voorlaadlijst), het verbod om het bestandstype te raden, een beperkte doorverwijzingsbron, en een insluitverbod voor andere websites behalve op de routes die uitdrukkelijk insluitbaar zijn.
- Bescherming tegen formulierverzending vanaf een andere website, met een uitdrukkelijke lijst van toegestane paden voor de koppeling met een leeromgeving.
- Snelheidsbegrenzing op circa 25 publieke eindpunten, met maatregelen tegen gelijktijdigheid, en met gezouten gehashte adressen in plaats van IP-adressen.
- Malwarecontrole van geüploade documenten vóór publicatie, met structurele opschoning van PDF's.

- Het vernieuwingstoken voor Google Classroom versleuteld opgeslagen (AES-256-GCM) met een aparte sleutel die alleen in de draaiende omgeving bestaat.
- Wachtwoorden van cursussen en van klasleden gehasht met scrypt en een eigen zout, vergeleken in constante tijd.
- Identiteiten uit de leeromgeving van een school opgeslagen als gehashte waarden; logregels tonen nooit de onbewerkte identiteit.
- Alle geheimen uit de instellingen van de draaiende omgeving; geen terugval op een bestand, geen geheim in het versiebeheer.
- Herbevestiging van het wachtwoord vóór verwijdering van het account en vóór een regiowijziging.
- Geplande taken beveiligd met een geheim, in constante tijd vergeleken, falend bij een ontbrekende waarde.

Punten die een Onderwijsinstelling expliciet moet meewegen

Het model vraagt om een beknopte, maar eerlijke opsomming. De volgende punten horen daarbij.

1. **Geüploade afbeeldingen, geluid en documenten zijn publiek leesbaar.** Zij krijgen een publieke URL in de objectopslag; wie de URL heeft, kan het bestand opvragen. Er is geen toegangscontrole op deze bestanden. De gepubliceerde leveranciersinformatie zegt dit ook: behandel materiaal in activiteiten als openbaar en zet er niets vertrouwelijks in.
2. **Een aantal gegevensonderdelen is bewust openbaar leesbaar**, omdat de spelpagina de inhoud rechtstreeks uit de database leest en niet via een server. Dat betreft de inhoud van een activiteit (per activiteit, niet per docent), het abonnementsniveau van de eigenaar, de vormgevingsvoorkeuren, de meerspelersessies, en — voor Puzzel LMS — de **weergavenamen op de klassenlijst**. Volledige namen, e-mailadressen en wachtwoordhashes van klasleden staan in een afgeschermd deel dat alleen de docent leest. Ook wereldwijd leesbaar zijn de koppeling docent → school en een individuele uitnodiging voor een schoolaccount (met naam en e-mailadres van afzender en ontvanger) voor wie de sleutel van die uitnodiging kent.
3. **Er is geen algemene Content-Security-Policy**, dat wil zeggen: geen regel die vastlegt welke scripts en welke bronnen een pagina mag laden. Alleen het insluitverbod voor andere websites en het afdwingen van een versleutelde verbinding zijn aanwezig. De meting met internet.nl van 20 september 2026 komt mede daardoor uit op 86%: het onderdeel HTTPS is volledig groen, maar onder "Beveiligingsopties" ontbreekt de Content-Security-Policy, en het domein is niet over IPv6 bereikbaar. Geen van beide raakt de versleuteling van het verkeer; beide staan hier omdat een school dezelfde test kan draaien.
4. **Er is geen tweefactorauthenticatie** in de applicatie zelf; een docent die met Google of Microsoft inlogt, neemt die van de aanbieder over. Een wachtwoord telt minimaal acht tekens: dat minimum is als wachtwoordbeleid in Firebase Authentication ingesteld, en de aanmeldpagina en het wachtwoordwijzigingsscherm noemen het ook.
5. **De toegangsregels worden met de hand in twee beheerconsoles geplaatst.** Er is één vastgelegde referentieversie van die regels; of beide regio's exact deze regels draaien, is een kwestie van discipline en moet worden gecontroleerd.
6. **Het back-upregime is beperkt**: dagelijkse back-ups van de database, geen back-up van geüploade bestanden en geen beproefde herstelprocedure (zie de rij "Back-up" hierboven).
7. **Geüploade foto's worden niet van metagegevens ontdaan.** Er is niets in de applicatie dat EXIF-gegevens — waaronder locatiegegevens — uit een geüploade foto verwijdert. Een foto van een schoolplein of een klas kan daarmee locatiegegevens dragen in een publiek opvraagbaar bestand. Dit is de feitelijke situatie op dit moment.
8. **Er is geen geautomatiseerde bouwstraat.** Er zijn wel eenheidstests — waaronder een testreeks tegen de toegangsregels van de database op een lokale emulator — en een typecontrole over de gehele software, maar niets voert ze vanzelf uit: er is geen omgeving die de tests automatisch draait, geen opdracht die alle tests achter elkaar uitvoert, en geen werkende automatische controle bij het vastleggen van een wijziging (de daarvoor aanwezige bestanden zijn restanten van een verwijderd hulpprogramma en doen niets). Elke test en de typecontrole worden

met de hand gestart, zodat een wijziging kan worden uitgerold zonder dat een test is gedraaid. Zie ook de rijen "Testen" en "Controle integriteit" hierboven.

9. **De tijdstempels op een resultaat zet de browser van de speler**, niet de server. Het tijdstip van aanmaken en het tijdstip van laatst spelen worden op de spelpagina op de klok van het apparaat gezet en zo naar de database geschreven; de toegangsregels toetsen alleen dát het een getal is, niet of het bij de tijd van de server in de buurt ligt. Alles wat beveiligings- of facturatierelevant is, draait wél op de klok van de server. Dit is geen lek, maar een school die resultaten gebruikt als bewijs dat op een bepaald moment is gewerkt, moet weten dat dat tijdstip niet onafhankelijk is vastgesteld.

Verwerker kan in plaats van het 'Certificeringsschema informatiebeveiliging en privacy ROSA' ook gebruikmaken van andere certificeringsmechanismen en/of (inter)nationaal erkende normen en standaarden voor informatiebeveiliging, mits die een gelijkwaardig of hoger niveau van beveiliging bieden en de door Verwerker genomen maatregelen aan de Onderwijsinstelling inzichtelijk worden gemaakt.

C. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Verwerker heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zal Verwerker de Verwerkingsverantwoordelijke de volgende informatie ter hand stellen:

- de kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk; samenvatting van de inbreuk, waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op welk onderdeel van de beveiliging heeft het betrekking, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van Persoonsgegevens);
- de oorzaak van de inbreuk;
- hoe de inbreuk is ontdekt;
- de maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;
- of de bij de inbreuk betrokken Persoonsgegevens versleuteld, gehasht etc. waren;
- de groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep(en) Betrokkenen;
- wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de groep(en) Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor de groep(en) Betrokkene(n);
- de hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere Persoonsgegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

In geval van een (vermoeden van een) beveiligingsincident en/of Datalek, kunnen Onderwijsinstelling en Verwerker in beginsel per e-mail contact met elkaar opnemen via onderstaande contactgegevens, dan wel de contactgegevens zoals opgenomen in Bijlage 4.

	Naam en functie contactpersoon bij beveiligingsincidenten/Datalekken	**Contactgegevens (e-mail en telefoonnummer)**
Verwerker	Daan Weustenraad, eigenaar. Er is geen tweede contactpersoon en geen escalatiepad; de gepubliceerde leveranciersinformatie vermeldt dit ook uitdrukkelijk. Er is geen vervanger bij afwezigheid.	daan@puzzel.org Er wordt geen telefoonnummer gepubliceerd; meldingen verlopen per e-mail.
Onderwijsinstelling	[In te vullen door de Onderwijsinstelling, of: zie Bijlage 4]	[Idem, of: zie Bijlage 4]

Meldtermijn. De Onderwijsinstelling wordt onverwijld geïnformeerd, en uiterlijk binnen 48 uur na ontdekking van de inbreuk, zodat zij een meldplichtig datalek binnen 72 uur bij de Autoriteit Persoonsgegevens kan melden.

Detectie. Er is geen actieve monitoring, geen alarmering en geen toegangslogboek. Een incident wordt in de praktijk opgemerkt door de eigenaar tijdens het dagelijkse beheer, door een melding van een gebruiker of een Onderwijsinstelling, of door een melding van een Subverwerker.

Bijlage 2 (Beveiligingsbijlage) maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad, de verschillende betrokken ketenpartijen (MEVW, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u op www.privacyconvenant.nl.

MODEL BIJLAGE 3: WIJZIGINGENBIJLAGE

INDIEN VAN TOEPASSING: VERPLICHTE BESCHRIJVING VAN DE NOODZAKELIJKE AFWIJKINGEN VAN DE MODEL VERWERKERSOVEREENKOMST

Verwerker: **Puzzel.org**. Versie **1.0**, datum laatste aanpassing **20 september 2026**.

Overzicht van afwijkingen, zoals bedoeld in artikel 14, lid 2 van de Model Verwerkersovereenkomst, en de motivering daarvan.

Stand van zaken

Partijen zijn geen wijzigingen overeengekomen. Deze bijlage bevat geen afwijkingen.

De tekst van de Model Verwerkersovereenkomst 4.0 wordt één op één overgenomen.

De doorgifte van Persoonsgegevens buiten de EER, die in onderdeel G van Bijlage 1 is beschreven, is géén afwijking van artikel 10 maar een toepassing ervan: artikel 10 lid 1 staat doorgifte toe mits de Onderwijsinstelling daarvoor specifieke schriftelijke toestemming geeft. Die toestemming wordt in onderdeel G van Bijlage 1 gevraagd en gegeven, en hoort daarom niet in deze bijlage thuis.

Vastlegging op grond van artikel 7 lid 4 (KetenID en Attributenset)

Artikel 7 lid 4 van de Model Verwerkersovereenkomst schrijft voor dat de Verwerker uitsluitend het KetenID en de toepasselijke Attributenset gebruikt bij alle Onderwijsdeelnemers die over een KetenID kunnen beschikken, en dat een Partij die hieraan redelijkerwijs niet kan voldoen dat **gemotiveerd in deze bijlage vastlegt**. Die vastlegging volgt hieronder. Zij is geen wijziging van de overeenkomst — de tekst van de artikelen blijft ongewijzigd — maar de door artikel 7 lid 4 zelf voorgeschreven melding.

Betreft artikel	Artikel 7 lid 4
Vastlegging	Puzzel.org gebruikt het KetenID en de bijbehorende Attributenset niet, en is niet aangesloten op de Nummervoorziening.
Hoe identificatie dan wel verloopt	Een Onderwijsdeelnemer speelt anoniem, of meldt zich aan met de registratievelden die de docent per activiteit zelf kiest, met een Google- of Microsoft-account van de school, via een klassenlijst die de docent aanlegt, of via een koppeling met de leeromgeving van de school volgens de LTI-standaard. In dat laatste geval komt de identiteit van de leeromgeving en wordt zij versleuteld tot een onomkeerbare waarde opgeslagen.
Motivering	Puzzel.org is een eenmanszaak en levert oefen- en toetsmateriaal, geen leerlingadministratie- of leerlingvolgsysteem. Aansluiting op de Nummervoorziening vergt een certificeringstraject en een doorlopende keteninspanning die niet in verhouding staan tot de omvang van de verwerking: er worden geen bijzondere persoonsgegevens en geen burgerservicenummers verwerkt, en de docent bepaalt per activiteit welke gegevens een Onderwijsdeelnemer überhaupt invult — vaak alleen een voornaam of een schuilnaam. Aansluiting is daarmee redelijkerwijs niet te vergen in de zin van artikel 7 lid 4.

Gevolg voor de Onderwijsinstelling	Een Onderwijsinstelling die het gebruik van het ECK iD verplicht stelt voor alle digitale leermiddelen, kan Puzzel.org niet onder die eis gebruiken. Dit punt staat hier zodat die afweging vóór ondertekening kan worden gemaakt.

Partijen zijn de volgende wijzigingen overeengekomen:

1. Beschrijving noodzakelijke afwijkingen Model Verwerkersovereenkomst

Betreft artikel	*(niet van toepassing — er zijn geen afwijkingen overeengekomen)*
Wijziging of aanvulling?	
Huidige tekst artikel	
Nieuwe tekst artikel (onderstreep wijzigingen en aanvullingen)	
Reden van wijziging of aanvulling (noodzaak en motivering)	

Bijlage 3 (Wijzigingenbijlage) maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad, de verschillende betrokken ketenpartijen (MEVW, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u op www.privacyconvenant.nl.