

Beveiligingsbijlage Penny Family

Bijlage 2 bij de Model Verwerkersovereenkomst 4.0. Versie 1.0 (concept), 9 oktober 2026. Beschrijft de technische en organisatorische maatregelen voor de app en de partneromgeving.

Penny Family is klein: twee makers, geen eigen servers. Daarom leunt een deel van de maatregelen op de subverwerkers (zie de privacybijsluit, onderdeel H). Waar een maatregel nog niet aantoonbaar op orde is, staat dat er eerlijk bij, met een plan.

A. Organisatorische maatregelen

Maatregel	Invulling
Beveiligingsbeleid dat periodiek wordt herzien	[IN TE VULLEN: kort beleidsdocument vaststellen, jaarlijks herzien]. Wel al: periodieke beveiligingsscan van code en database (juli en augustus 2026), met een logboek van bevindingen en oplossingen
Toegang op basis van rol	Alleen de twee makers hebben beheertoegang. Medewerkers van een school zien alleen hun eigen partneromgeving. Kinderen kunnen niet bij elkaars gegevens en communiceren met niemand
Coördinator informatiebeveiliging	[IN TE VULLEN: naam]
Registratie van beveiligingsincidenten	Bevindingen en oplossingen worden bijgehouden in een beveiligingslogboek in de broncode
Communicatie over incidenten	Zie onderdeel C
Geheimhouding van medewerkers	[IN TE VULLEN: geheimhoudingsafpraak tussen de makers en met eventuele hulpkrachten]
Bewustwording en training	[IN TE VULLEN]

Artikel 32 AVG. Versleuteling van verbindingen en opslag, toegangscontrole, het vermogen om na een incident de beschikbaarheid te herstellen (zie B, herstel) en periodieke toetsing van de maatregelen. Wat daarvan nog open staat, staat in onderdeel B.

B. Technische maatregelen

BIV-classificatie (voorstel): Beschikbaarheid **Laag**, Integriteit **Midden**, Vertrouwelijkheid **Midden**. Toelichting: het gaat om gegevens over kinderen, maar zonder bijzondere persoonsgegevens, zonder BSN en zonder financiële gegevens; de school ziet alleen totalen. Uitval raakt geen onderwijsproces dat niet kan wachten.

Categorie	Maatregel	Status	Toelichting
Beschikbaarheid: ontwerp	Beheerde database en hosting, geen eigen servers	Alternatieve maatregel	Capaciteit en onderhoud van de infrastructuur liggen bij Supabase
Beschikbaarheid: testen	Automatische tests en controles bij elke build	Voldaan	Unit- en end-to-end-tests, plus controles die de build tegenhouden bij fouten
Beschikbaarheid: monitoring	Foutmeldingen en logs	Alternatieve maatregel	Foutregistratie (Sentry) alleen voor volwassenen met toestemming, nooit tijdens kindsessies; daarnaast de logs van Supabase
Beschikbaarheid: herstel	Back-up en hersteltest	Niet voldaan	Nog niet aangetoond. Correctieplan: back-upinstellingen van de database vastleggen en één keer een hersteltest doen [IN TE PLANNEN]
Integriteit: herleidbaarheid	Wijzigingen in de database via vastgelegde migraties in versiebeheer	Voldaan	
Integriteit: applicatiecontroles	De server bepaalt munten en voortgang, met een maximum per dag	Voldaan	Kinderen kunnen hun eigen voortgang niet vervalsen
Vertrouwelijkheid: logische toegang	Rijbeveiliging (RLS) op alle tabellen met kindgegevens; pincodes van kinderen gehasht (bcrypt); blokkade na vijf foute pogingen; sessies met een niet te vervalsen token	Voldaan	Gecontroleerd tegen de draaiende database op 9 augustus 2026
Vertrouwelijkheid: inlogblokkade per bron	Blokkade telt per adres én per naam, zodat iemand anders een kind niet uit de app kan houden	Niet voldaan (op 9 augustus 2026)	Staat klaar als database-aanpassing, moest nog worden uitgevoerd. [TE CONTROLEREN of dit inmiddels live staat]

Vertrouwelijkheid: sessies intrekken	Bij het wijzigen van een pincode vervallen bestaande sessies	Niet voldaan	Correctieplan: databasewijziging, afgestemd op de uitgebrachte app [IN TE PLANNEN]
Vertrouwelijkheid: fysieke toegang	Datacenter van de subverwerker	Alternatieve maatregel	Supabase, EU (Ierland)
Vertrouwelijkheid: netwerk	TLS op alle verbindingen, HSTS, strikte Content Security Policy zonder externe scripts	Voldaan	
Vertrouwelijkheid: clickjacking	Header die voorkomt dat de site in een frame wordt geladen	Niet voldaan	Ligt bij de hosting; verzoek aan de host staat klaar
Vertrouwelijkheid: transport en opslag	Versleuteld verkeer; opslag in een beheerde database met versleuteling in rust	Voldaan	Versleuteling in rust door Supabase [TE CONTROLEREN in de documentatie van Supabase]
Vertrouwelijkheid: scheiding omgevingen	Gescheiden test- en productieomgeving	[TE CONTROLEREN]	
Vertrouwelijkheid: geheimen	Geen geheime sleutels in de app of broncode; alleen publieke sleutels	Voldaan	Geheime sleutels staan als secrets bij de server
Vertrouwelijkheid: kwetsbaarheden	Periodieke scan van code, pakketten en database	Voldaan	Laatste scan in het logboek: 9 augustus 2026
Vertrouwelijkheid: dataminimalisatie	Geen tracking bij kinderen, geen advertenties, school ziet alleen totalen vanaf vijf gezinnen	Voldaan	

Toetsingsmethode: zelfevaluatie door Penny Family, 9 oktober 2026, op basis van het beveiligingslogboek. [IN TE VULLEN: naam en functie van de beoordelaar.] Het normenkader is ROSA, het certificeringsschema informatiebeveiliging en privacy uit het convenant; een externe toets is er nog niet.

C. Incidenten en datalekken

Procedure.

1. Wie een (mogelijk) beveiligingsincident ziet, meldt het direct bij de contactpersoon beveiliging (zie de tabel hieronder).
2. Penny Family beperkt de schade (bijvoorbeeld sessies intrekken, een functie uitzetten) en zoekt uit wat er is gebeurd.
3. Gaat het om persoonsgegevens uit de partneromgeving, dan meldt Penny Family dit zo snel mogelijk aan de school, binnen de termijn van de Model Verwerkersovereenkomst, zodat de school zelf kan beoordelen of een melding bij de Autoriteit Persoonsgegevens of aan betrokkenen nodig is.
4. Penny Family legt elk incident vast, ook als het geen datalek blijkt, en gebruikt dat om maatregelen te verbeteren.

Wat de melding aan de school bevat: wanneer het lek plaatsvond en hoe lang het duurde; wat er is gebeurd en de oorzaak; hoe het is ontdekt; wat er is gedaan om het te stoppen en de gevolgen te beperken; of de gegevens versleuteld of gehasht waren; welke groepen betrokken zijn en om hoeveel mensen het gaat; de waarschijnlijke gevolgen; welke soorten gegevens en hoeveel.

Partij	Naam	Functie	E-mail	Telefoon
Penny Family	[IN TE VULLEN]	Contactpersoon beveiliging	info@pennyfamily.nl	[IN TE VULLEN]
Onderwijsinstelling	In te vullen door de school			