



Protocol Privacy & AVG

Gezinshuis De Hoeksteen

Versie 1.0 | Geldig vanaf: 1 oktober 2025 | Herzien uiterlijk: 1 oktober 2027

Verwerkingsverantwoordelijke: Gezinshuis De Hoeksteen

1. Doel en reikwijdte

Dit protocol beschrijft hoe Gezinshuis De Hoeksteen voldoet aan de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) bij de verwerking van persoonsgegevens van jeugdigen, ouders/verzorgers, wettelijk vertegenwoordigers, medewerkers, vrijwilligers, stagiairs en bezoekers. Het protocol geldt voor alle verwerkingen, zowel digitaal als op papier, inclusief cameratoezicht, e-mail, apps en uitwisseling met ketenpartners (bijv. Enver, gemeenten, jeugdbescherming, onderwijs, huisarts).

2. Begrippen (samenvatting)

- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
- Bijzondere persoonsgegevens: o.a. gegevens over gezondheid, strafrechtelijke gegevens (alleen in uitzonderlijke gevallen).
- Verwerkingsverantwoordelijke: Gezinshuis De Hoeksteen (tenzij schriftelijk anders overeengekomen).
- Verwerker: partij die namens ons persoonsgegevens verwerkt (bijv. softwareleverancier, cloudprovider).
- Betrokkene: jeugdige, ouder/verzorger, medewerker e.d.
- Datalek: inbreuk op de beveiliging die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking/toegang.

3. Rollen en verantwoordelijkheden

- Gezinshuisouders / Directie: eindverantwoordelijk voor naleving AVG, vaststelling beleid en toekennen middelen.
- Privacycontact / Functionaris gegevensbescherming (indien aangewezen): adviseert, monitort, ondersteunt datalekafhandeling en DPIA's.
- Medewerkers/vrijwilligers: voeren beleid uit, volgen werkafspraken en melden (vermoedelijke) datalekken direct.

- Enver (plaatsingen via zorgaanbieder): afzonderlijk verwerkingsverantwoordelijke voor haar systemen/processen; gegevensuitwisseling volgens samenwerkings- en/of verwerkersafspraken.
- Gemeente/voogd (maatwerkcontracten): regievoerder of gezamenlijke verwerkingsverantwoordelijke voor het jeugdhulptraject waar van toepassing; gegevensuitwisseling volgens (gezamenlijke) verwerkingsafspraken.
- Verwerkers: uitsluitend met verwerkersovereenkomst (art. 28 AVG), inclusief subverwerkers, beveiliging en datadoorgifte.

4. Rechtsgrondslag en doelen

Wij verwerken persoonsgegevens op basis van:

- Wettelijke verplichting en publieke taak binnen de Jeugdwet (dossiervorming, gegevensuitwisseling in het zorgtraject).
- Uitvoering van een overeenkomst (zorg-/plaatsingsovereenkomst, arbeidsovereenkomst).
- Gerechtvaardigd belang (beveiliging van eigendommen en personen, o.a. cameratoezicht – na belangenafweging).
- Toestemming (alleen waar nodig en passend; intrekbaar).

Doelen zijn o.a.: leveren van zorg en begeleiding; dossiervorming en rapportage; declaratie en administratie; kwaliteitsverbetering; beveiliging; werving & selectie; communicatie.

5. Categorieën gegevens en systemen

- Identificatie- en contactgegevens (naam, adres, contact).
- Gevoelige gegevens: gezondheidsgegevens, ontwikkel-/gedragsinformatie, ondersteuningsplannen, rapportages.
- Beeld- en geluidsgegevens van cameratoezicht (alleen gemeenschappelijke ruimten, geen privéruimtes).
- IT-systemen: [invullen, bijv. Enver/Zilliz dossier, e-mail, cloudopslag, boekhouding].

6. Bewaartermijnen

- Jeugdhulpdossier: minimaal 20 jaar na einde hulp, tenzij langer noodzakelijk. (Jeugdwet)
- Camerabeelden: zo kort mogelijk en nooit langer dan noodzakelijk (richtlijn: max. 28 dagen), langer alleen bij incident tot afhandeling.
- HR/financieel: volgens fiscale termijnen (bijv. 7 jaar).
- Sollicitaties: 4 weken na einde procedure, of max. 1 jaar met toestemming.
- Overige bewaartermijnen: zie Bijlage A – Verwerkingsregister & Bewaartermijnen.

7. Rechten van betrokkenen

- Inzage en kopie; rectificatie; beperking; dataportabiliteit (waar van toepassing).
- Vernietiging van gegevens: conform Jeugdwet/AVG, met wettelijke uitzonderingen (bijv. dossiervorming in jeugdhulp).
- Bezwaar tegen verwerkingen op basis van gerechtvaardigd belang (bijv. cameratoezicht).
- Verzoeken binnen 1 maand afhandelen; identiteit verifiëren; register bijhouden van verzoeken.

8. Beveiliging (organisatorisch & technisch)

- Toegangsbeheer: 'least privilege', unieke accounts, sterke wachtwoorden, MFA voor primaire systemen.
- Apparaten & opslag: versleuteling op laptops/telefoons, schermvergrendeling, geen privacygevoelige data op privéapparatuur zonder autorisatie.
- E-mail & delen: gebruik van versleutelde overdracht voor gevoelige info; geen WhatsApp voor dossierinformatie.
- Logging & monitoring: beveiligingslogs bewaren en beoordelen; periodieke kwetsbaarheidsscan (indien mogelijk).
- Fysieke beveiliging: afgesloten dossierruimten; schoon-bureaubeleid; shredden van papier.
- Leveranciersbeheer: due diligence, verwerkersovereenkomsten, subverwerkers alleen met toestemming.
- Opleiding & bewustwording: jaarlijkse AVG/NEN-7510 bewustwording voor medewerkers.

9. Cameratoezicht (alleen indien noodzakelijk)

- Doel: veiligheid van jeugdigen/medewerkers en bescherming eigendommen in algemene ruimten; nooit in badkamers/slaapkamers/toiletten.
- DPIA: uitvoeren vooraf; alternatieven en proportionaliteit aantonen; betrokkenen informeren (pictogram + privacyinformatie).
- Bewaartermijn: kort en noodzakelijk (richtlijn: max. 28 dagen), langer enkel bij incidenten tot afhandeling.
- Toegang beelden: strikt geautoriseerd; logging van raadpleging; geen live-volgen tenzij strikt noodzakelijk.
- Periodieke evaluatie: doelmatigheid en noodzaak jaarlijks herbeoordelen; documenteer besluit.

10. Datalekken (melden binnen 72 uur indien meldplichtig)

- Definities & voorbeelden: verlies USB, verkeerd geadresseerde e-mail, hack, ransomware, onbevoegde inzage.
- Direct melden intern bij privacycontact/directie; registreer in Datalekregister (Bijlage B).
- Beoordeling risico's; zo nodig melding Autoriteit Persoonsgegevens (AP) binnen 72 uur; zo nodig betrokkenen informeren.
- Herstelmaatregelen documenteren en evalueren; lessons learned opnemen in scholingsplan.

11. DPIA & privacy by design/default

- DPIA uitvoeren bij (kans op) hoog risico, o.a. structurele monitoring, grootschalige verwerking van gevoelige gegevens, systematisch cameratoezicht, kinderdatabank.
- Resultaten DPIA implementeren; bij onaanvaardbaar risico vooraf overleg met AP ('prior consultation').
- Nieuwe systemen/leveranciers alleen na privacy- en security-check en passende contracten.

12. Gegevensdeling met ketenpartners

- Alleen delen wat noodzakelijk is ('need-to-know'), met een wettelijke grondslag of overeenkomst/toestemming.
- Gebruik van veilige kanalen; leg vast in dossier welke gegevens met wie en waarom zijn gedeeld.
- Voor Enver-plaatsingen: werkafspraken conform Enver-beleid; voor gemeentelijke maatwerkcontracten: afspraken met regievoerder/voogd.
- Internationale doorgifte: uitsluitend binnen EER of met passende waarborgen (SCC's/IDTA).

13. Relevante procedures (koppeling)

- Meldcode Huiselijk Geweld en Kindermishandeling (separaat protocol).
- Incidenten- en klachtenprocedure (AKJ/Jeugdteam).
- Informatiebeveiligingsbeleid en toegangsbeheer.
- Camera-protocol (indien van toepassing).

14. Versiebeheer en evaluatie

- Dit protocol wordt minimaal elke 2 jaar geëvalueerd en na incidenten/aanpassingen tussentijds geactualiseerd.
- Eigenaarschap: Gezinshuisouders/Directie; wijzigingen worden gecommuniceerd aan alle medewerkers en ketenpartners waar relevant.

Bijlage A – Verwerkingsregister (samenvatting) & bewaartermijnen

Verwerking	Categorie persoonsgegevens	Doel & grondslag	Ontvangers/verwerkers	Bewaartermijn	DPIA nodig?
Cliëntdossier jeugdhulp	Identificatie, gezondheid, begeleidingsgegevens	Publieke taak Jeugdwet/overeenkomst	Enver/gemeente/jeugdbescherming/onderwijs/huisarts (waar nodig)	Minimaal 20 jaar na einde hulp	Ja/nee – afhankelijk van omvang/risico
Camera toezicht (algemene ruimten)	Beeldgegevens bezoekers/jeugdigen/medewerkers	Gerechtigd belang (beveiliging)	Beheerder camerasysteem / beveiligingsbedrijf (verwerker)	Max. 28 dagen; langer bij incident tot afhandeling	DPIA uitvoeren vooraf
HR & salaris	Persoons- en loonheffingsgegevens	Wettelijke plicht/overeenkomst	Salarisverwerker/boekhouder (verwerker)	Fiscale termijnen (min. 7 jaar)	Nee
Sollicitaties	Contact- en CV-gegevens	Gerechtigd belang/Toestemming	N.v.t.	4 weken; 1 jaar met toestemming	Nee

Bijlage B – Datalekregister (template)

Datum/ontdekker	Omschrijving incident	Betrokken gegevens/antal	Risico-inschatting	Meldingen (AP/betrokkenen)	Maatregelen/afhandeling

Bijlage C – Formulieren rechten betrokkenen

C1. Verzoek tot inzage/kopie (naam, relatie, identificatie, welk dossier, reden)

C2. Verzoek tot rectificatie/aanvulling (omschrijving onjuistheid en gewenste wijziging)

C3. Verzoek tot beperking/verzet (reden bezwaar; verwerkingen waarop bezwaar ziet)

C4. Verzoek tot vernietiging (Jeugdwet/AVG – voor zover toegestaan, met afweging wettelijke bewaarplichten)

Bijlage D – Cameratoezicht: informatiebord & privacy-informatie (voorbeeld)

- Doel: beveiliging personen/eigendommen. • Verwerkingsverantwoordelijke: Gezinshuis De Hoeksteen.
- Contact: [gezinshuisdehoeksteen@protonmail.com/+31 6 52606603 & +31 6 41971146].
- Rechtsgrond: gerechtvaardigd belang (AVG art. 6 lid 1 f).
- Bewaartermijn: max. 28 dagen, langer bij incident.
- Rechten: inzage, bezwaar, beperking; zie privacyinformatie.
- **Geen** camera's in privéruimten.

Bijlage E – Verwerkersovereenkomst (checklist art. 28 AVG)

- Onderwerp en duur van de verwerking; aard en doel; soort persoonsgegevens en categorieën betrokkenen.
- Verplichtingen verwerker (geheimhouding, passende beveiliging, datalekmeldingen, assistentie bij rechten).
- Subverwerkers alleen met voorafgaande toestemming; zelfde verplichtingen doorleggen.
- Doorgifte buiten EER uitsluitend met passende waarborgen (SCC's).
- Teruggave/vernietiging na einde diensten; audits en inzage in relevante informatie.