

# *PRIVACY POLICY*



## *KINDERDAGVERBLIJF TOPPIE*

*HENDRIK SMITSTRAAT 10 A*

*HILVERTSWEG 162 A*

*HOLLEWEG 1*

*OPGESTELD DOOR: V.H. VOS & L.M SCHIPPER  
& TOPPIE TEAM*

*OPGESTELD TE: HILVERSUM*

*DATUM: FEBRUARI 2018*

*LAATST GEWIJZIGD: FEBRUARI 2018*

## Voorwoord

Voor u ligt het privacy beleid van kinderopvangorganisatie Toppie. Dit beleid is opgesteld in februari 2018 ten behoeve van de Algemene Verordening Gegevensbescherming. Dit beleid is tot stand gekomen met de tool, voor ons beschikbaar gesteld door de Branchevereniging Kinderopvang.

Toppie hecht veel waarde aan de bescherming van uw persoonsgegevens. In deze Privacy Policy willen we heldere en transparante informatie geven over hoe wij omgaan met persoonsgegevens.

Wij doen er alles aan om uw privacy te waarborgen en gaan daarom zorgvuldig om met persoonsgegevens. Toppie houdt zich in alle gevallen aan de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming. Dit brengt met zich mee dat wij in ieder geval:

- Uw persoonsgegevens verwerken in overeenstemming met het doel waarvoor deze zijn verstrekt, deze doelen en type persoonsgegevens zijn beschreven in deze Privacy Policy;
- Verwerking van uw persoonsgegevens beperkt is tot enkel die gegevens welke minimaal nodig zijn voor de doeleinden waarvoor ze worden verwerkt;
- Vragen om uw uitdrukkelijke toestemming als wij deze nodig hebben voor de verwerking van uw persoonsgegevens;
- Passende technische en organisatorische maatregelen hebben genomen zodat de beveiliging van uw persoonsgegevens gewaarborgd is;
- Geen persoonsgegevens doorgeven aan andere partijen, tenzij dit nodig is voor uitvoering van de doeleinden waarvoor ze zijn verstrekt;
- Op de hoogte zijn van uw rechten omtrent uw persoonsgegevens, u hierop willen wijzen en deze respecteren.

Als Toppie zijn wij verantwoordelijk voor de verwerking van uw persoonsgegevens. Indien u na het doornemen van ons Privacy Policy, of in algemenere zin, vragen heeft hierover of contact met ons wenst op te nemen kan dit via de contactgegevens onder aan dit document.

## INVENTARISATIE PERSOONSgegevens

Wij bewaren de volgende 'gewone' persoonsgegevens, van zowel medewerkers die voor onze organisatie werken, ouders en kinderen die bij onze organisatie kinderopvang afnemen.

Naam  
Voorletters  
Tussenvoegsel  
Adres  
Postcode  
Woonplaats  
Provincie  
Land  
Telefoonnummer  
E-mailadres  
Geslacht  
Geboortedatum  
Bankrekeningnummer

Wij bewaren de volgende 'bijzondere' persoonsgegevens, van zowel medewerkers die voor onze organisatie werken, ouders en kinderen die bij onze organisatie kinderopvang afnemen.

Gegevens over gezondheid (kinderen met een allergie o.i.d.)  
Salarisgegevens (van onze medewerkers, niet van de ouders)  
Paspoort kopie, waarop pasfoto zichtbaar is (van onze medewerkers, niet van de ouders)  
BSN nummer (van de ouders en de kinderen en onze medewerkers)

Alle bovenstaande gegevens staan in ons planningsprogramma, of staat beschreven op desbetreffende formulieren, of delen wij met onze salarisadministratie, of delen wij met de belastingdienst.

## INVENTARISATIE DOELBINDING

Wij verwerken de volgende persoonsgegevens met onderstaande doelen, daar hebben wij ze voor gekregen en uitsluitend daarvoor gebruiken wij deze. Dat noemen we 'doelbinding'. Het is belangrijk dat persoonsgegevens alleen worden verwerkt (opgeslagen en gebruikt) voor de doeleinden waarvoor deze zijn verkregen.

Grondslag: Grondslag is een reden op basis waarvan de persoonsgegevens verwerkt mogen worden. Een reden voor ons is dat wij deze persoonsgegevens nodig hebben voor het uitvoeren van de plaatsingsovereenkomst.

### Ouders en kinderen: BSN

Organisaties buiten de overheid mogen het BSN (burger-servicenummer) alleen gebruiken als dat volgens de wet is toegestaan.

Persoonsgegevens	naam + adres + woonplaats + telefoonnummer + email + BSN + geboortedatum + bankgegevens
Grondslag	overeenkomst met handtekening op papier (persoonlijk gegevens formulier en machtiging automatische incasso)
Doel	ouders moeten kinderopvangtoeslag aanvragen bij de overheid, ter controle van deze kinderopvangtoeslag moeten wij bij de belastingdienst de KOI gegevens aanleveren, waaronder het BSN nummer van alle kinderen en hun ouders
Verwerkingen	interactie met de overheid in het belang van (en met toestemming van) de ouders
Verwerking door	afdeling administratie
ICT systeem	planningsprogramma
Bewaartermijn	gedurende de duur van de overeenkomst, indien aan alle betalingsverplichtingen zijn voldaan

### Kinderen

Gezondheidsgegevens	gegevens m.b.t. ontwikkeling, allergieën, medicijngebruik etc.
Grondslag	formulier bijzonderheden / medicijnverstrekkingformulier / observatielijsten
Doel	ontwikkeling en gezondheid waarborgen van het kind
Verwerkingen	medewerkers op de groep van het betreffende kind
Verwerking door	afdeling administratie en medewerkers
ICT systeem	nvt
Bewaartermijn	gedurende de duur van de overeenkomst, indien aan alle betalingsverplichtingen zijn voldaan

### Medewerkers

Persoonsgegevens	naam + adres + woonplaats + telefoonnummer + email + BSN + geboortedatum + salarisgegevens + kopie ID + bankgegevens
Grondslag	arbeidsovereenkomst

Doel	wij hebben de gegevens van de medewerkers nodig om aan te leveren voor de salarisverwerking
Verwerkingen	salariëring
Verwerking door	afdeling administratie en accountant
ICT systeem	via accountant
Bewaartermijn	gedurende de duur van de overeenkomst

#### VERSTREKKING AAN DERDEN

De gegevens die u aan ons geeft kunnen wij aan derde partijen verstrekken indien dit noodzakelijk is voor uitvoering van de hierboven beschreven doeleinden.

Zo maken wij gebruik van een derde partij voor:

- Het verzorgen van de internetomgeving van het planningsprogramma;
- Het verzorgen van de (financiële en salaris) administratie;
- Het verzorgen van nieuwsbrieven en uitnodigingen;
- Het verzorgen van de internetomgeving voor het mailprogramma;
- Het aanleveren van gegevens aan de belastingdienst

Wij geven nooit persoonsgegevens door aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten. Met deze partijen (verwerkers) maken wij hierin uiteraard de nodige afspraken om de beveiliging van uw persoonsgegevens te waarborgen. Verder zullen wij de door uw verstrekte gegevens niet aan andere partijen verstrekken, tenzij dit wettelijk verplicht en toegestaan is. Een voorbeeld hiervan is dat de politie in het kader van een onderzoek (persoons)gegevens bij ons opvraagt. In een dergelijk geval dienen wij medewerking te verlenen en zijn dan ook verplicht deze gegevens af te geven. Tevens kunnen wij persoonsgegevens delen met derden indien u ons hier schriftelijk toestemming voor geeft.

#### BEVEILIGING

Wij hebben passende technische en organisatorische maatregelen genomen om persoonsgegevens van u te beschermen tegen onrechtmatige verwerking, zo hebben we bijvoorbeeld de volgende maatregelen genomen;

- Alle personen die namens TOPPIE van uw gegevens kennis kunnen nemen, zijn gehouden aan geheimhouding daarvan
- We hanteren een gebruikersnaam en wachtwoordbeleid op al onze systemen;
- Wij maken back-ups van de persoonsgegevens om deze te kunnen herstellen bij fysieke of technische incidenten;
- We testen en evalueren regelmatig onze maatregelen;

Onze medewerkers zijn geïnformeerd over het belang van de bescherming van persoonsgegevens

## RECHTEN OMTRENT PERSOONLIJKE GEGEVENS

Iedereen heeft recht op inzage, rectificatie of verwijdering van de persoonsgegevens welke wij hebben. Tevens kan er bezwaar gemaakt worden tegen de verwerking van deze persoonsgegevens (of een deel hiervan) door ons of door een van onze verwerkers. Ook heeft iedereen het recht de verstrekte gegevens door ons te laten overdragen aan welke partij dan ook indien gewenst. Wij kunnen logischerwijs vragen om legitimatie voordat wij gehoor kunnen geven aan voornoemde verzoeken.

## VERWERKERSOVEREENKOMST

Wij hebben met de volgende partijen een verwerkersovereenkomst;

Atomos; zij ontwikkelen en beheren ons planningsprogramma  
V13; zij beheren onze website en onze mail  
MTH; zij verzorgen onze boekhouding en onze salarisadministratie  
Rabobank; geregeld via de PSD 2 wet  
ING bank; geregeld via de PSD 2 wet

## TOEGANGSBEVEILIGING

Wij hebben verschillende toegangssystemen bij de ingangen van de locaties, deze systemen zijn voldoende beveiligd.

## SOFTWARE

Onze software is veilig en altijd up to date.

## GEGEVENS BUITEN DE EU

Wij slaan geen gegevens op buiten de EU.

## GEAUTORISEERDE MEDEWERKERS

Er zijn in onze organisatie 3 personen geautoriseerd voor toegang tot alle persoonsgegevens van cliënten van Toppie, de twee eigenaren en de vestigingsmanager, waarvan laatstgenoemde een geheimhouding heeft ondertekend. De digitale toegang tot persoonsgegevens is altijd beveiligd met een inlogcode en een wachtwoord en de papieren toegang tot persoonsgegevens is alleen mogelijk op het kantoor aan de Holleweg, waarvan genoemde 3 personen in het bezit zijn van een sleutel.

Voor alle medewerkers toegankelijk zijn slechts de persoonsgegevens die ervoor zorgen dat de verzorging van de kinderen optimaal kan worden uitgevoerd en dat er contact kan opgenomen worden in daarvoor nodige situaties. Deze gegevens zijn de bijzonderheden, de medische gegevens en de naam van het kind en de telefoonnummers van de ouders.

## MINDERJARIGEN

Wij verwerken enkel en alleen persoonsgegevens van minderjarigen (personen jonger dan 16 jaar) indien daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.

## VERNIETIGEN PERSOONSgegevens

Toppie bewaart persoonsgegevens niet langer dan noodzakelijk voor het doel waarvoor deze zijn verstrekt dan wel op grond van de wet is vereist.

Wij vernietigen de volgende (digitale) gegevens:

- Gegevens uit het planningsprogramma
- Plaatsingsovereenkomst (als alle betalingen zijn voldaan)
- Machtiging automatische incasso
- Formulier persoonlijke gegevens
- Formulieren medicijnverstrekking
- Formulier bijzondere gegevens
- Formulier registratie ongevallen

## DATALEK

Een datalek is een inbreuk op de beveiliging van persoonsgegevens. Een datalek is een beveiligingsincident waarbij persoonsgegevens gelekt zijn. Dit kan gaan om een ongeoorloofde toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens. Van een datalek is alleen sprake als er persoonsgegevens zijn gelekt!

Enkele voorbeelden van datalekken om dit wat duidelijker te maken:

- Je raakt een USB-stick met daarop persoonsgegevens kwijt
- Er is een laptop gestolen met daarop persoonsgegevens
- Er is door een hacker ingebroken in een databestand of systeem (met daarop persoonsgegevens)
- Er is een mailing verstuurd met alle e-mailadressen in de Aan of CC in plaats van BCC
- Uit een tas zijn papieren gestolen met daarop persoonsgegevens
- Door een crash van een harddisk of door brand zijn persoonsgegevens verloren gegaan en er is geen back-up

In bepaalde gevallen ben je verplicht melding te doen van een datalek bij de Autoriteit Persoonsgegevens ([www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl)). Ook kan het zo zijn dat je de betrokkenen moet informeren over het datalek. Dit zijn de personen van wie je gegevens verwerkt. Meld je een datalek niet terwijl je dit volgens de wet wel had moeten doen? Dan kan de Autoriteit Persoonsgegevens je een (flinke) boete geven. Ook is het belangrijk dat je alle datalekken vastlegt. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of je aan de meldplicht hebt voldaan.

Als er binnen Toppie een datalek optreedt is het belangrijk dat je de juiste actie onderneemt. Je moet direct aan de slag en mogelijk moet je het incident binnen 72 uur melden bij de Autoriteit Persoonsgegevens. In sommige gevallen moet je ook de betrokkenen informeren.

## MEDEWERKERS, BEWUSTWORDING EN GEDRAG

Alle medewerkers hebben de video van de stichting AVG bekeken, zij hebben deze Privacy Policy doorgenomen en deze wordt jaarlijks besproken tijdens de teamvergadering.

Do's en dont's:

We hebben praktische tips voor wat medewerkers wel en niet moeten doen. Hieronder vind je een lijstje.

- Blokkeer altijd je beeldscherm bij het verlaten van je werkplek;
- Laat documenten met persoonsgegevens nooit onbeheerd achter op je bureau of bij de printer;
- Kies nooit voor automatisch opslaan van inloggegevens op je computer;
- Besef dat openbare netwerken niet veilig zijn;
- Let op wat je deelt via sociale media;
- Bedek altijd je webcam om 'meekijken' te voorkomen;
- Gebruik nooit de inlog van een collega en geef je inloggegevens ook niet door aan een collega;
- Zorg ervoor dat je mobiele telefoon beveiligd is met een inlogcode of vingerherkenning.