PRIVACY BELEID

THEO POUW GROEP

INHOUDSOPGAVE

1. Inleiding 3

2. Definities, rollen en verantwoordelijkheden 4

2.1. Definities 4
2.2. Rollen en verantwoordelijkheden 4

3. Verwerking van persoonsgegevens 6

3.1. Regels bij de verwerking van persoonsgegevens 6
3.2. Grondslagen bij verwerking van persoonsgegevens 6
3.3. Bijzondere persoonsgegevens 7

4. Rechten van betrokkenen 8

4.1. Rechten 8
4.2. Privacyverklaring 8
4.3. Verzoeken uitvoering rechten 8

5. Beveiliging 11

5.1. Beveiliging personeelsgegevens 11

6. Datalekken 12

6.1. Procedure datalekken 12
6.2. Datalek bij verwerker 12

7. Verwerkers 13

7.1. Overeenkomsten met verwerkers 13
7.2. Subverwerker 13
7.3. Register van verwerkingen 13
7.4. Doorgifte persoonsgegevens aan derde landen 14

8. Bewaartermijnen 15

8.1. Verwerkingen bij indiensttreding 15
8.2. Verwerking bij ziekte 15
8.3. Bewaartermijn personeelsdossiers 16

9. Gegevenseffectbeoordeling 17

1. Inleiding

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze Europese privacywetgeving heeft als doel de persoonsgegevens van burgers binnen de Europese Unie beter te beschermen en organisaties meer verantwoordelijkheid te geven bij het verwerken van persoonsgegevens. De AVG vervangt de eerdere privacywetgeving en stelt strengere eisen aan hoe organisaties omgaan met persoonlijke gegevens.

De Theo Pouw Groep gaat zorgvuldig om met persoonsgegevens. Wij vinden het belangrijk om de privacy van onze klanten, medewerkers en andere relaties te beschermen. Van onze medewerkers en externe partners verwachten wij dat zij vertrouwelijk omgaan met persoonsgegevens.
Bij het werken met persoonsgegevens gebruiken wij de volgende privacy principes:

1. Bewaar gegevens veilig.
2. Deel informatie alleen als dat nodig is.
3. Respecteer de privacy van iedereen.
4. Meld een (mogelijk) datalek direct bij de aangewezen collega.
5. Zorg dat mensen hun privacy rechten kunnen gebruiken.

In dit privacy beleid wordt uitgelegd hoe de Theo Pouw Groep omgaat met persoonsgegevens en op welke manier wij voldoen aan de eisen van de Algemene Verordening Gegevensbescherming.

Dit beleid is vastgesteld door de directie van de Theo Pouw Groep en treedt in werking per 1 oktober 2026. Hiermee worden alle voorgaande interne beleidsstukken met betrekking tot verwerking van persoonsgegevens en privacy vervangen. Dit beleid kan door de directie van de Theo Pouw Groep worden aangepast.

2. Definities, rollen en verantwoordelijkheden

2.1. Definities

- AP: De Nederlandse autoriteit persoonsgegevens, de toezichthouder op de naleving van de AVG.
- Betrokkene: De natuurlijke persoon op wie een persoonsgegeven betrekking heeft.
- Bijzondere persoonsgegevens: Persoonsgegevens die iemands godsdienst, ras, politieke overtuiging, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod betreffen.
- Datalek: Een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of waarbij een onrechtmatige verwerking niet redelijkerwijs kan worden uitgesloten.
- Theo Pouw Groep: Theo Pouw Beheer bv en gelieerde ondernemingen
- Persoonsgegevens: Elk gegeven dat betrekking heeft op een geïdentificeerde of identificeerbare natuurlijke persoon.
- Subverwerker: Een partij die door de verwerker is aangewezen en in diens opdracht persoonsgegevens verwerkt.
- Toezichthoudende autoriteit: De AP, of een andere toezichthoudende autoriteit van een EU-lidstaat die verantwoordelijk is voor toezicht op grond van de AVG.
- Verwerking van persoonsgegevens: Elke handeling of reeks handelingen met persoonsgegevens, zoals verzamelen, vastleggen, ordenen, bewaren, wijzigen, raadplegen, gebruiken, verstrekken of vernietigen.
- Verwerker: Degene die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke, zonder onder diens gezag te staan. De verwerkingsverantwoordelijke bepaalt de middelen en doeleinden van de verwerking.

2.2. Rollen en verantwoordelijkheden

2.2.1 Directieverantwoordelijke gegevensbescherming

De eindverantwoordelijkheid voor de bescherming van persoonsgegevens ligt bij de directieverantwoordelijke voor gegevensbescherming (Marga Pouw), in haar afwezigheid bij een aangestelde vervanger op directieniveau.

Taken:

- Zorgt voor effectief gegevensbeschermingsbeleid en toezicht op beheer, toetsing en verantwoording.
- Integreert privacy in bestaande managementsystemen voor kwaliteits- en certificeringsdoeleinden.
- Beslist over het melden van beveiligingsincidenten bij de Toezichthoudende Autoriteit en fungeert als woordvoerder.
- Wordt geïnformeerd wanneer betrokkenen hun privacy rechten uitoefenen.

2.2.2 Privacy team

Het privacy team is het team dat de directieverantwoordelijke voor gegevensbescherming ondersteunt bij het beheer en de doorontwikkeling van het privacy-managementsysteem. Het team bestaat uit vertegenwoordigers van HR, KAM, PR, IT en Finance en heeft de expertise het privacy management van de Theo Pouw Groep te ondersteunen.

Taken:

- Beheert operationeel het privacy-managementsysteem van de organisatie.
- Adviseert en controleert het privacy-managementsysteem; onderhoudt administratie zoals beleid, privacy verklaringen, verwerkersovereenkomsten, datalekprocedures en verwerkingsregister.
- Voert operationele controles uit en stelt rapportages op om te tonen dat de organisatie “in control” is op het gebied van gegevensbescherming.
- Is contactpersoon voor betrokkenen die hun privacy rechten uitoefenen en zorgt voor correcte afhandeling binnen 4 weken (maximaal verlengbaar tot 8 weken) na toestemming van de directieverantwoordelijke.
- Toetst periodiek of gegevensverwerking voldoet aan de beginselen van gegevensbescherming en rapporteert aan de directie; brengt bevindingen onder de aandacht van directie en medewerkers.
- Volgt procedures bij mogelijke beveiligingsincidenten, onderzoekt deze en informeert de directieverantwoordelijke.

- Draagt zorg voor meldingen aan de Toezichthoudende Autoriteit, alleen na toestemming van de directieverantwoordelijke.
- Komt vier keer per jaar bijeen voor overleg; er worden notulen bijgehouden.

2.2.3 Medewerkers

Alle medewerkers van de Theo Pouw Groep zijn verplicht om op een zorgvuldige wijze conform de beleidsregels en principes van de Theo Pouw Groep de verplichtingen uit de AVG met persoonsgegevens om te gaan.

Taken:

- Binnen het eigen taakgebied verantwoordelijk voor het naleven van deze principes.
- Melden en herkennen mogelijke incidenten die kunnen leiden tot een datalek.
- Het bewust nalaten incidenten te melden is een reden voor (mogelijke) sancties.

2.2.4 De toezichthouder AP

De Theo Pouw Groep en de door haar ingeschakelde verwerkers werken altijd mee aan de AP of, als dat nodig is, een andere toezichthouder en geven binnen redelijke en afgesproken termijnen antwoord op informatieverzoeken

3. Verwerking van persoonsgegevens

Bij de Theo Pouw Groep worden alle gegevens die direct of indirect terug te leiden zijn naar een natuurlijk persoon gezien als persoonsgegeven. Gegevens over personenvennootschappen horen ook bij natuurlijk personen. Een rechtspersoon zelf hoort hier niet bij. Als de vertegenwoordiger van de rechtspersoon een natuurlijk persoon is, valt deze persoon wel onder persoonsgegevens. Alleen levende personen kunnen rechten uitoefenen volgens de AVG.

Persoonsgegevens worden bij de Theo Pouw Groep op verschillende manieren op papier en digitaal verwerkt. In het verwerkingsregister van de Theo Pouw Groep staan ook, als dat nodig is, de applicaties die worden gebruikt voor het opslaan en verwerken van persoonsgegevens.

3.1. Regels bij de verwerking van persoonsgegevens

Bij de Theo Pouw Groep worden persoonsgegevens verwerkt volgens de AVG. Dit betekent:

- Persoonsgegevens worden op een legale, eerlijke en duidelijke manier verwerkt.
- Persoonsgegevens worden alleen verzameld voor een duidelijk doel en mogen niet voor iets anders gebruikt worden.
- Alleen de persoonsgegevens die nodig zijn voor het doel worden gebruikt.
- Persoonsgegevens moeten correct zijn en worden zo nodig aangepast of verwijderd.
- Persoonsgegevens worden niet langer bewaard dan nodig is, volgens het retentiebeleid.
- Persoonsgegevens worden beschermd tegen verlies, diefstal en misbruik door goede technische en organisatorische maatregelen.

De Theo Pouw Groep is verantwoordelijk voor het naleven van deze regels en kan aantonen dat ze worden gevolgd. De Theo Pouw Groep kan aantonen dat deze regels worden nageleefd.

3.2. Grondslagen bij verwerking van persoonsgegevens

Bij de Theo Pouw Groep mogen persoonsgegevens alleen verwerkt worden als er een grondslag voor is. Dit betekent dat persoonsgegevens verwerkt mogen worden als:

- Persoonsgegevens nodig zijn om een contract uit te voeren.
- Persoonsgegevens nodig zijn om te voldoen aan een wettelijke verplichting.
- Persoonsgegevens nodig zijn voor een gerechtvaardigd belang van de Theo Pouw Groep, zolang dit niet belangrijker is dan de rechten van de persoon. De directie van de Theo Pouw Groep kan, eventueel met advies van het privacy team, besluiten gegevens te verwerken voor een zwaarwegend gerechtvaardigd belang van het bedrijf. Voorbeelden zijn marketing, het voorkomen van fraude, witwassen of belastingontduiking. Voor minderjarigen zal deze grondslag nooit gebruikt worden.
- De persoon toestemming geeft, deze toestemming kan altijd worden ingetrokken.
- Persoonsgegevens nodig zijn om het leven of de gezondheid van iemand te beschermen.

De directie van de Theo Pouw Groep, op advies van het privacy team, mag toestemming van de klant gebruiken als basis voor het verwerken van persoonsgegevens. Als de directie toestemming geeft, moet aan de volgende regels worden voldaan:

- Er moet duidelijk bewijs zijn dat de betrokkene toestemming heeft gegeven voor het verwerken van zijn of haar persoonsgegevens.
- Als toestemming schriftelijk wordt gevraagd in een verklaring die ook over andere onderwerpen gaat, moet in eenvoudige taal duidelijk staan waar de toestemming precies voor is.
- Een gegeven toestemming kan altijd weer worden ingetrokken. Vooraf wordt de klant/persoon hierover geïnformeerd. Het intrekken moet net zo makkelijk zijn als het geven van toestemming. Als toestemming wordt ingetrokken, geldt dit alleen voor de toekomst, niet voor het verleden.
- Betrokkene jonger dan 16 jaar mogen zelf geen toestemming geven. In dat geval moeten de ouders of verzorgers toestemming geven. De Theo Pouw Groep probeert, als dat redelijk mogelijk is, te controleren of de ouder of verzorger echt toestemming heeft gegeven.

3.3. Bijzondere persoonsgegevens

In noodzakelijke gevallen worden door de Theo Pouw Groep bijzondere persoonsgegevens verwerkt. Bij nieuwe medewerkers wordt bij indiensttreding gecontroleerd op betrouwbaarheid. Dit gebeurt via een VOG-verklaring. Voor sommige functies kan dit aangevuld worden met een uitgebreidere screening. Hierbij wordt de achtergrond en relevante werkervaring zorgvuldig gecontroleerd om de betrouwbaarheid en integriteit binnen de Theo Pouw Groep te waarborgen. Bijzondere persoonsgegevens kunnen ook verwerkt worden om vitale belangen van de betrokkene te beschermen of om verplichtingen en rechten van de Theo Pouw Groep of de betrokkene uit te voeren op het gebied van arbeidsrecht en sociale zekerheid, mits dit toegestaan is volgens de Nederlandse wet of een geldende collectieve arbeidsovereenkomst.

4. Rechten van betrokkenen

4.1. Rechten

Iedere betrokkene van wie gegevens worden verwerkt heeft de volgende rechten:

- Je mag zien welke gegevens er van jou zijn opgeslagen (artikel 15 AVG).
- Je mag fouten in je gegevens laten corrigeren (artikel 16 AVG).
- Je mag vragen dat je gegevens worden verwijderd (artikel 17 AVG).
- Je mag vragen dat je gegevens minder worden gebruikt (artikel 18 AVG).
- Je mag je gegevens in een handig formaat ontvangen en overdragen (artikel 20 AVG).
- Je mag bezwaar maken tegen het gebruik van je gegevens (artikel 21 AVG).

Als je één van deze rechten wilt gebruiken, zal het privacy team je verzoek binnen de tijd en regels van de AVG behandelen.

4.2. Privacyverklaring

De rechten die hierboven staan, maakt de Theo Pouw Groep aan de betrokkene duidelijk via de privacyverklaring voor kandidaten, medewerkers, leveranciers en klanten. Op werknemers in dienst van de Theo Pouw Groep is daarnaast de “Privacyverklaring Theo Pouw Groep’’ van toepassing. Als de Theo Pouw Groep persoonsgegevens van andere partijen ontvangt, zal de Theo Pouw Groep aan de aanvullende informatieverplichtingen voldoen. De privacyverklaring is duidelijk en makkelijk te begrijpen. Als de betrokkene dit wil, kan de Theo Pouw Groep de informatie ook mondeling geven. Dit kan alleen als de identiteit van de persoon is bewezen.

Op de website van de Theo Pouw Groep staat de actuele privacyverklaring. De privacyverklaring wordt regelmatig beoordeeld en aangepast als dat nodig is. In de privacyverklaring wordt in ieder geval de volgende informatie opgenomen:

- De entiteit en contactgegevens van de Theo Pouw Groep;
- De redenen waarvoor persoonsgegevens worden gebruikt en de wettelijke basis voor de verwerking;
- Als persoonsgegevens worden verwerkt op basis van gerechtvaardigde belangen, wordt aangegeven welke belangen dat zijn;
- Met wie de persoonsgegevens worden gedeeld of wie toegang heeft tot de gegevens;
- De periode waarvoor persoonsgegevens worden bewaard. Als dit niet precies kan worden aangegeven, staan de criteria voor het bepalen van de bewaartermijn vermeld;
- De rechten van betrokkenen;
- De mogelijkheid om een klacht in te dienen bij de AP;
- Of het verplicht is persoonsgegevens te verstrekken, bijvoorbeeld voor een contract of vanwege de wet, en wat er gebeurt als gegevens niet worden verstrekt;
- Als persoonsgegevens voor een ander doel worden gebruikt dan waarvoor ze zijn verzameld, wordt hierover informatie gegeven en worden andere relevante gegevens gedeeld.

4.3. Verzoeken uitvoering rechten

Een betrokkene kan vragen om zijn of haar rechten uit te oefenen. De Theo Pouw Groep behandelt dit verzoek, behalve als de Theo Pouw Groep de betrokkene niet kan identificeren. Bij twijfel over de identiteit vraagt de Theo Pouw Groep om extra informatie om de identiteit te controleren.

De betrokkene verstuurt het verzoek naar privacy@theopouw.nl. Het privacy team behandelt het verzoek. Het privacy team informeert de directieverantwoordelijke voor gegevensbescherming over elk ontvangen verzoek. Het privacy team behandelt het verzoek uit binnen vier weken na ontvangst. Een verzoek dat digitaal is ontvangen, mag ook digitaal worden beantwoord. Dit is anders als de betrokkene vraagt om een afschrift in hard copy. Soms lukt het niet het verzoek binnen vier weken te behandelen, bijvoorbeeld omdat het verzoek ingewikkeld is of omdat er veel verzoeken zijn. In dat geval kan de termijn met acht weken worden verlengd. Hiervoor is vooraf toestemming nodig van de directieverantwoordelijke voor gegevensbescherming.

De betrokkene krijgt binnen vier weken na ontvangst van het verzoek bericht over deze verlenging. Het kan zijn dat de Theo Pouw Groep het verzoek niet uitvoert. De directieverantwoordelijke voor gegevensbescherming besluit hierover, eventueel op advies van het privacy team. De betrokkene krijgt binnen vier weken na ontvangst van het verzoek uitleg over dit besluit. Ook wordt uitgelegd dat de betrokkene een klacht kan indienen bij de AP of naar de rechter kan gaan.

Het behandelen van verzoeken van de betrokkene is kosteloos. De directieverantwoordelijke voor gegevensbescherming kan wel besluiten dat:

- Er een redelijke vergoeding wordt gevraagd als iemand steeds opnieuw een verzoek doet of als het verzoek tijdrovend is;
- Het verzoek niet wordt uitgevoerd als er geen goede reden voor is.

4.3.1 Verzoek tot inzage

De betrokkene heeft het recht om te weten of zijn of haar persoonsgegevens worden verwerkt. Als dat zo is, mag de betrokkene deze persoonsgegevens inzien. De Theo Pouw Groep geeft bij een verzoek tot inzage een kopie van de persoonsgegevens die worden verwerkt. De betrokkene krijgt ook informatie over:

- Het doel van de verwerking;
- De categorieën persoonsgegevens die worden verwerkt;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens;
- De bewaartermijn van de persoonsgegevens of de criteria om deze termijn te bepalen;
- Het recht van de betrokkene om persoonsgegevens te laten verwijderen, de verwerking te beperken of bezwaar te maken tegen de verwerking;
- Het recht om een klacht in te dienen bij de AP.

4.3.2 Verzoek tot correctie

De betrokkene kan de Theo Pouw Groep vragen om persoonsgegevens te corrigeren als deze niet juist of niet volledig zijn. Als de Theo Pouw Groep het verzoek goedkeurt, wordt de betrokkene hierover geïnformeerd.

4.3.3 Verzoek tot verwijdering

De betrokkene heeft het recht om de Theo Pouw Groep te vragen om zijn of haar persoonsgegevens te verwijderen. Als de Theo Pouw Groep het verzoek goedkeurt, worden de gegevens zo snel mogelijk verwijderd en krijgt de betrokkene hierover bericht. Dit gebeurt in ieder geval als:

- De persoonsgegevens niet meer nodig zijn voor het doel waarvoor ze zijn verzameld of verwerkt.
- De betrokkene zijn of haar toestemming heeft ingetrokken en er geen andere reden is om de gegevens te verwerken.
- De betrokkene bezwaar heeft gemaakt tegen de verwerking en er geen zwaarder belang is om de gegevens toch te verwerken.
- De persoonsgegevens onrechtmatig zijn verwerkt.
- De persoonsgegevens volgens Europese of nationale wetgeving moeten worden verwijderd.

De directieverantwoordelijke voor gegevensbescherming kan een verzoek tot verwijdering weigeren als de gegevens nodig zijn voor het instellen, uitoefenen of onderbouwen van een rechtsvordering.

4.3.4 Verzoek tot overdracht

De betrokkene kan vragen om zijn of haar persoonsgegevens over te laten dragen. Het privacy team behandelt dit verzoek als:

- Het gaat om persoonsgegevens die de betrokkene zelf heeft verstrekt.
- De verwerking is gebaseerd op toestemming of op een overeenkomst.

De Theo Pouw Groep zorgt ervoor dat de gegevens worden verstrekt in een gestructureerde, gangbare en voor computers leesbare vorm.

4.3.5 Verzoek tot beperking

De betrokkene kan vragen om de verwerking van persoonsgegevens tijdelijk te beperken. Dit kan in de volgende situaties:

- De betrokkene twijfelt of dat de persoonsgegevens juist zijn. De verwerking wordt dan beperkt zolang dit wordt onderzocht.
- De verwerking is onrechtmatig, maar de betrokkene verzoekt niet om verwijderingen maar om beperking van het gebruik van de gegevens .
- De Theo Pouw Groep heeft de persoonsgegevens niet meer nodig, maar de betrokkene heeft ze nodig voor een rechtsvordering.
- De betrokkene heeft bezwaar gemaakt tegen de verwerking en wacht op het antwoord van de Theo Pouw Groep.

4.3.6 Recht van bezwaar

De betrokkene heeft het recht om bezwaar te maken tegen de verwerking van persoonsgegevens als deze worden verwerkt op basis van het gerechtvaardigd belang van de Theo Pouw Groep. De directieverantwoordelijke voor gegevensbescherming kan, na advies van het privacy team, besluiten dat het bezwaar niet wordt goedgekeurd als er een zwaarder belang is om de gegevens toch te verwerken. Als persoonsgegevens worden gebruikt voor direct marketing, wordt een bezwaar van de betrokkene altijd goedgekeurd. De verwerking wordt dan gestopt.

5. Beveiliging

De Theo Pouw Groep zorgt ervoor dat persoonsgegevens worden beschermd. Hierbij wordt rekening gehouden met de huidige techniek, de kosten, de risico's en het soort gegevens. Er worden passende technische en organisatorische maatregelen genomen om persoonsgegevens te beschermen tegen verlies, vernietiging, vervalsing, ongewenste toegang, verspreiding of ander misbruik. De Theo Pouw Groep heeft hiervoor een apart IT-beleid.

De Theo Pouw Groep zorgt ervoor dat bij het verwerken van persoonsgegevens rekening wordt gehouden met:

- De huidige techniek;
- De uitvoeringskosten;
- De aard, de omvang, de context en het doel van de verwerking;
- De kans en ernst van risico's voor de rechten en vrijheden van personen.

5.1. Beveiliging personeelsgegevens

Alle persoonsgegevens worden veilig bewaard, zoals beschreven. Alleen de directie en HR-medewerkers mogen deze gegevens bekijken. Managers mogen alleen toegang krijgen tot gegevens van hun eigen medewerkers, en alleen als dat echt nodig is voor hun werk als leidinggevende.

6. Datalekken

6.1. Procedure datalekken

Een datalek wordt behandeld en gedocumenteerd volgens de procesbeschrijvingen zoals opgenomen in de procedure meldplicht datalekken.

Als er bij de Theo Pouw Groep een inbreuk op persoonsgegevens plaatsvindt, wordt deze gebeurtenis altijd geregistreerd. De directieverantwoordelijke voor gegevensbescherming bepaalt, met advies van het privacy team, of er sprake is van een datalek en of betrokkenen moeten worden geïnformeerd. Als er sprake is van een datalek, meldt het privacy team dit zo snel mogelijk, en uiterlijk binnen 72 uur nadat de inbreuk bij de Theo Pouw Groep bekend is geworden, bij de AP. Dit gebeurt na toestemming van de directieverantwoordelijke voor gegevensbescherming. Een melding is niet nodig als het waarschijnlijk is dat de inbreuk geen risico vormt voor de rechten en vrijheden van personen. Als de melding niet binnen 72 uur kan worden gedaan, legt de Theo Pouw Groep aan de AP uit waarom de melding later is gedaan. Als de inbreuk een hoog risico vormt voor de rechten en vrijheden van betrokkenen, zorgt de Theo Pouw Groep ervoor dat deze personen zo snel mogelijk worden geïnformeerd. Als er een uitzondering uit de AVG geldt waardoor betrokkenen niet geïnformeerd hoeven te worden, wordt er geen melding gedaan.

6.2. Datalek bij verwerker

Als er een datalek bij de verwerker plaatsvindt, moet de verwerker het privacy team van de Theo Pouw Groep direct informeren. Daarbij geeft de verwerker de volgende informatie:

- Wat er is gebeurd, welke soorten persoonsgegevens en betrokkenen het betreft en een schatting van de aantallen;
- De naam en contactgegevens van de functionaris voor gegevensbescherming of een andere contactpersoon;
- De mogelijke gevolgen van het datalek;
- De maatregelen die zijn genomen of voorgesteld om het lek te verhelpen en de schade te beperken.

Wanneer niet alle gegevens bekend zijn, kan de verwerker alvast de beschikbare informatie doorgeven. De Theo Pouw Groep zorgt ervoor dat alle informatie over het datalek wordt vastgelegd, zodat de AP dit kan controleren.

7. Verwerkers

De Theo Pouw Groep werkt in de bedrijfsvoering met verschillende verwerkers. Deze worden bij uitbesteding aangesteld volgens de uitgangspunten voor uitbesteding binnen de Theo Pouw Groep. De Theo Pouw Groep mag alleen verwerkers selecteren die kunnen aantonen dat zij passende technische en organisatorische maatregelen nemen. Zo wordt voldaan aan de eisen van de AVG en blijven de rechten van betrokkenen beschermd.

7.1. Overeenkomsten met verwerkers

De Theo Pouw Groep gebruikt een standaard verwerkersovereenkomst als basis. Afhankelijk van de situatie wordt de overeenkomst van de Theo Pouw Groep of die van de verwerker gebruikt. De directie van de Theo Pouw Groep zorgt samen met het privacy team dat elke opdracht voor het verwerken van persoonsgegevens in een aparte overeenkomst wordt vastgelegd. In deze overeenkomst staan in elk geval de volgende afspraken:

- De verwerker verwerkt persoonsgegevens alleen op schriftelijke instructie van de Theo Pouw Groep. De Theo Pouw Groep bepaalt of doorgifte aan landen buiten de EU of internationale organisaties is toegestaan, behalve als de wet anders verplicht. In dat geval meldt de verwerker dit aan de Theo Pouw Groep, tenzij de wet dit verbiedt.
- Personen die namens de verwerker gegevens verwerken, hebben een geheimhoudingsplicht.
- De verwerker neemt passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen (volgens artikel 32 AVG).
- De verwerker volgt dit beleid als hij een andere verwerker inschakelt.
- De verwerker helpt, waar redelijk mogelijk, bij het behandelen van verzoeken van betrokkenen over hun rechten.
- De verwerker helpt bij het naleven van de AVG-verplichtingen, zoals beveiliging, het melden van datalekken aan de AP of de betrokkene, en het uitvoeren van een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment = DPIA). Een datalek moet direct, maar uiterlijk binnen 24 uur, aan de Theo Pouw Groep worden gemeld.
- Na afloop van de dienstverlening verwijdert of vernietigt de verwerker alle persoonsgegevens, tenzij de wet bewaarplicht oplegt.
- De verwerker werkt mee aan controles en audits door de Theo Pouw Groep of een derde partij om aan te tonen dat hij de regels naleeft.
- De verwerker werkt alleen volgens de instructies van de Theo Pouw Groep en verwerkt niet meer gegevens dan nodig is voor de opdracht.
- De verwerker werkt mee aan redelijke verzoeken van de Theo Pouw Groep of de AP, zoals het laten zien van het register van verwerkingsactiviteiten.

7.2. Subverwerker

Als de verwerker (een deel van) het werk wil laten doen door een andere subverwerker, moet hij hiervoor eerst schriftelijke toestemming vragen aan de Theo Pouw Groep. Als de verwerker bij het afsluiten van de overeenkomst al subverwerkers gebruikt, moet hij op verzoek van de Theo Pouw Groep aangeven welke partijen dit zijn. De verwerker zorgt ervoor dat de afspraken zoals genoemd in paragraaf 7.1 ook in de overeenkomst met de subverwerker worden opgenomen. Daarbij blijft de verwerker altijd verantwoordelijk en aansprakelijk voor het werk van de subverwerker.

7.3. Register van verwerkingen

De Theo Pouw Groep zorgt dat alle verwerkingen van persoonsgegevens van de Theo Pouw Groep in een verwerkingsregister worden vastgelegd. Het verwerkingsregister wordt schriftelijk of digitaal bijgehouden In dit register staan in ieder geval:

- De naam en contactgegevens van de Theo Pouw Groep en van de directieverantwoordelijke voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van betrokkenen en persoonsgegevens;
- De categorieën ontvangers van de gegevens, inclusief eventuele ontvangers in derde landen;

- Indien relevant: of persoonsgegevens worden doorgegeven aan derde landen;
- Indien mogelijk de bewaartermijn;
- Indien mogelijk een algemene beschrijving van de technische en organisatorische maatregelen om persoonsgegevens te beveiligen.

De Theo Pouw Groep zorgt er ook voor dat verwerkers een register bijhouden van alle verwerkingen die zij in opdracht van de Theo Pouw Groep uitvoeren. In dit register staan in ieder geval:

- De naam en contactgegevens van de Theo Pouw Groep en van de directieverantwoordelijke voor gegevensbescherming;
- De categorieën van verwerkingen die voor de Theo Pouw Groep worden uitgevoerd;
- Indien van toepassing: doorgifte van persoonsgegevens aan een derde land, met vermelding van dat land en de passende waarborgen;
- Indien van toepassing: een beschrijving van de technische maatregelen om persoonsgegevens te beschermen.

7.4. Doorgifte persoonsgegevens aan derde landen

De Theo Pouw Groep zorgt ervoor dat persoonsgegevens niet naar landen buiten de EU of EER worden gestuurd als die landen geen goede bescherming hebben. Als persoonsgegevens toch naar een ander land worden gestuurd, controleert het privacy team altijd naar welk land. Het privacy team beslist of extra maatregelen nodig zijn om de gegevens veilig te houden. Het privacy team mag persoonsgegevens naar andere landen sturen op basis van adequaatheidsbesluiten, op basis van passende waarborgen, dan wel op basis van bindende bedrijfsvoorschriften onder voorwaarden toe te laten.

8. Bewaartermijnen

Bij de Theo Pouw Groep worden persoonsgegevens niet langer bewaard dan nodig is. In het verwerkingsregister staat per verwerking hoe lang gegevens worden bewaard. Persoonsgegevens worden altijd minimaal zo lang bewaard als de wet voorschrijft, vanaf het sluiten van het dossier. Omdat er kans is op een rechtszaak, kunnen dossiers langer worden bewaard. Het privacy team maakt samen met de directieverantwoordelijke richtlijnen voor bewaartermijnen. De directieverantwoordelijke voor gegevensbescherming kan samen met de afdeling HR en IT extra beveiliging voor deze gegevens regelen.

Werknemers worden ook verwezen naar de Privacy Verklaring Theo Pouw Groep.

8.1. Verwerkingen bij indiensttreding

Een sollicitant wordt volgens het beleid gecontroleerd op betrouwbaarheid. Bij indiensttreding worden persoonsgegevens verwerkt om de indiensttreding correct af te handelen. Tijdens de arbeidsovereenkomst verwerkt de Theo Pouw Groep de persoonsgegevens van medewerkers om te voldoen aan verplichtingen uit de arbeidsovereenkomst. Dit gebeurt bijvoorbeeld voor:

- Salarisbetaling en declaraties
- Ziek- en betermeldingen
- Pensioenafspraken
- Opleidingen en trainingen
- Tijdregistratie
- Contact met deurwaarders of overheidsinstanties
- Nieuwsbrieven
- Verzekeringen namens werknemers

Daarnaast worden persoonsgegevens gebruikt voor planning, coaching en beoordeling van medewerkers.
De verwerkingen zijn gebaseerd op het naleven van wettelijke verplichtingen of de uitvoering van de (arbeids)overeenkomst. Soms is dit ook op basis een gerechtvaardigd belang van de Theo Pouw Groep, wanneer dit zwaarder weegt dan het belang van de medewerker.

8.2. Verwerking bij ziekte

Als een werknemer zich ziekmeldt, mag de Theo Pouw Groep alleen gegevens gebruiken die nodig zijn om te kijken of er recht is op doorbetaling van loon en wanneer de werknemer weer kan werken. Het is wel toegestaan om informatie over chronische ziekten te bewaren als dat belangrijk is voor het geven van eerste hulp, maar niet over medicijnen. Ook mag de Theo Pouw Groep bijhouden hoe lang iemand ziek is en of de ziekte verband heeft met de Theo Pouw Groep

Er wordt nooit gevraagd naar de oorzaak of soort ziekte. Als een werknemer vrijwillig over zijn ziekte praat, wordt die informatie niet in het personeelsdossier gezet of op een andere manier opgeslagen.

De Theo Pouw Groep mag controleren of een werknemer echt ziek is, zodat duidelijk is of het loon doorbetaald moet worden. Zo'n controle gebeurt alleen als er duidelijke aanwijzingen zijn dat de werknemer niet ziek is en kan werken. In dat geval mag de Theo Pouw Groep een vroegtijdige oproep naar de Arbodienst sturen. Er wordt geen recherchebureau of andere dienst ingeschakeld, tenzij er een heel zwaarwegende reden is.

Aan de Arbodienst worden alleen deze gegevens doorgegeven:

- Persoonsgegevens van de werknemer;
- Informatie die de werknemer bij ziekmelding geeft en wat de Arbodienst zelf observeert.

Het ziekteverzuimdossier wordt maximaal twee jaar bewaard nadat de werknemer uit dienst is.

De directie zorgt ervoor dat alleen enkele medewerkers toegang hebben tot het externe verzuimsysteem, namelijk HR-medewerkers en de direct leidinggevende. In dit systeem wordt het verzuim geregistreerd.

8.3. Bewaartermijn personeelsdossiers

De Theo Pouw Groep houdt personeelsdossiers bij met de belangrijke gegevens van medewerkers. Deze gegevens worden bewaard zolang dat nodig is, maar niet langer dan de termijnen die staan in het retentiebeleid voor personeelsdossiers.

De directie die verantwoordelijk is voor gegevensbescherming kan beslissen dat sommige gegevens een andere bewaartermijn krijgen. Gegevens die niet meer nodig zijn, worden veilig en volgens de wet verwijderd.

9. Gegevenseffectbeoordeling

De directieverantwoordelijke voor gegevensbescherming kan, op advies van het privacy team, beslissen dat er een DPIA nodig is voor verwerkingen met hoog risico. Het privacy team kijkt daarbij naar de richtlijnen van het comité (art. 68 AVG) en de AP.

Ook al verwerkt de Theo Pouw Groep geen gegevens waarvoor volgens de AVG een DPIA verplicht is, wordt regelmatig gecontroleerd of een DPIA toch nodig is. De directie wijst iemand aan die de DPIA uitvoert. Het privacy team zorgt dat de DPIA actueel blijft en minstens eens in de drie jaar wordt herzien.

Als uit een DPIA blijkt dat een verwerking een hoog risico heeft en er geen goede maatregelen zijn, moet de Theo Pouw Groep in overleg gaan met de AP. Bij dit overleg geeft de Theo Pouw Groep de volgende informatie aan de AP:

- Wie verantwoordelijk is voor de verwerking en de betrokken verwerkers;
- Wat het doel van de verwerking is en hoe het gebeurt;
- Welke maatregelen worden genomen om de rechten van betrokkenen te beschermen;
- De contactgegevens van de directieverantwoordelijke voor gegevensbescherming;
- De DPIA zelf;
- Andere informatie die de AP vraagt.