Privacystatement St. Anna Advies B.V.

1. Introductie

Dit is het privacybeleid van St. Anna Advies B.V. (hierna: SAA), gevestigd en kantoorhoudende aan St. Annastraat 404, 6525 ZM te Nijmegen. Dit privacybeleid ziet op het verzamelen en verwerken van persoonsgegevens van cliënten. Het privacybeleid beschrijft op welke wijze SAA met deze gegevens omgaat en welke protocollen en processen zij heeft geïmplementeerd om ervoor te zorgen dat de veiligheid van de gegevens gewaarborgd is en dat aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) wordt voldaan.

In dit privacybeleid komen de volgende onderwerpen aan bod:

- Verwerkingsregister
- Type persoonsgegevens en doelen
- Informatieplicht
- Rechten van betrokkenen
- Derde partijen
- Beveiliging
- Datalekken
- Bewaartermijnen
- Doorgifte van persoonsgegevens
- Functionaris Gegevensbescherming

Om ervoor te zorgen dat dit privacybeleid blijft aansluiten bij de verwerking van persoonsgegevens binnen SAA, zal het privacybeleid worden geëvalueerd. Aan de hand van die evaluatie zal, indien vereist, het privacybeleid en de hieraan gehechte protocollen en documenten worden aangepast. Indien op een moment voor de evaluatie duidelijk wordt dat het privacybeleid aanpassing behoeft, zal SAA de vereiste aanpassingen doorvoeren.

2. Definities

Verwerker
(Degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.)

➔ SAA is als Verwerker aan te merken.

Externe verwerker
(Een externe partij die ten behoeve van de Verwerker persoonsgegevens verwerkt.)

➔ Bijvoorbeeld, maar niet uitsluitend: Google G Suite, MailChimp, Google Analytics.

Persoonsgegevens
(Alle gegevens die direct of indirect tot een persoon te herleiden zijn.)

➔ Hieronder vallen bijvoorbeeld NAW-gegevens, telefoonnummer en e-mailadres.

FG
(Functionaris Gegevensbescherming

➔ Voor SAA is dit Matthijs Heijstek

3. Privacybeleid

3.1. Verwerkingsregister

SAA houdt een verwerkingsregister bij. Dit register bevat onder meer een beschrijving van de (categorieën) persoonsgegevens die binnen SAA worden verwerkt, de doelen waarvoor ze worden verwerkt, de derden aan wie de gegevens worden verstrekt, de bewaartermijn van de gegevens en de technische en organisatorische maatregelen die zijn genomen om de gegevens te beschermen.

In het verwerkingsregister wordt voor elke verwerking opgenomen welke persoonsgegevens worden verzameld en voor welk doel ze worden gebruikt. Voorbeelden van gegevensverwerkingen zijn:

- Het registreren van persoonsgegevens in ons CRM-systeem om een nieuwe (potentiële) klant in te schrijven.

- Het vastleggen en bijhouden van persoonsgegevens van een contactpersoon van een organisatie die producten/diensten afneemt bij SAA, ten behoeve van onder andere facturatie, het maken van afspraken en het toesturen van producten.

Binnen SAA hebben alle medewerkers toegang tot het register. Het register wordt door SAA continu en actief bijgehouden. Wijzigingen in de verwerking van persoonsgegevens worden direct in het register doorgevoerd.

3.2. Types persoonsgegevens en doeleinden

Binnen SAA worden persoonsgegevens van potentiële (a) en bestaande (b) klanten verwerkt.

a) Potentiële klanten

Wanneer een medewerker van een organisatie die nog geen klant is bij SAA per telefoon of e-mail contact opneemt met SAA, worden een aantal gegevens van deze contactpersoon en de organisatie waar hij/zij werkt verwerkt. De informatie die SAA opneemt in haar administratie betreft: NAW-gegevens van de organisatie, volledige naam van contactpersoon, en een telefoonnummer en e-mailadres waarop de contactpersoon gecontacteerd wil worden (dit mag zakelijke of privé zijn).

Indien iemand via het contactformulier op de website van SAA (www.anna-advies.nl) een bericht stuurt, komt dit bericht binnen in een van de mailboxen. De naam en het e-mailadres uit het contactformulier zullen (ongeacht de aard van het bericht) eenmalig in de mailbox van SAA worden verwerkt, met als reden om naar aanleiding van het gestuurde bericht contact op te kunnen nemen met de zender, via de ingevulde contactgegevens.

b) Bestaande klanten

Onder ‘bestaande klanten’ worden partijen verstaan die producten en/of diensten (willen) afnemen bij SAA. Van deze partijen worden, naast de NAW-gegevens van de organisatie, ook de volledige naam van de contactpersoon, en een telefoonnummer en e-mailadres waarop de contactpersoon van de organisatie gecontacteerd wil worden (dit mag zakelijke of privé zijn) verwerkt in het CRM-systeem.

In het CRM-systeem worden ook de facturen en offertes voor klanten opgesteld. SAA verzendt facturen en offertes standaard per e-mail naar het opgegeven e-mailadres van klanten, tenzij een klant expliciet aangeeft een factuur/offerte op andere wijze te willen ontvangen.

Voor het maken van afspraken, heeft SAA de optie om klanten een online datumplanner te laten invullen. Deze datumplanner is volledig in eigen beheer van SAA.

Alle gegevens die over klanten worden verzameld, worden gebruikt met als doel een duidelijk en correct contact met klanten te kunnen onderhouden. Daarnaast kan het voorkomen dat SAA producten per post opstuurt naar klanten. Ook gebruiken wij het opgegeven e-mailadres en/of de opgegeven NAW-gegevens voor het verzenden van bijvoorbeeld onze nieuwsbrief. SAA maakt geen gebruik van geautomatiseerde besluitvorming.

3.3. Rechtsgronden

SAA verwerkt persoonsgegevens in ieder geval op basis van grondslag 1 van de AVG: “Toestemming van de betrokken persoon”, en indien van toepassing (mede) op basis van grondslag 2: “Noodzakelijk voor de uitvoering van een overeenkomst”.

3.4. Informatieplicht

SAA stelt nieuwe klanten bij inschrijving op de hoogte van de persoonsgegevens die zij over de klant verzamelt en voor welke doeleinden deze persoonsgegevens vervolgens worden gebruikt. Dit doet SAA door het Privacystatement St. Anna Advies B.V. en de Algemene Voorwaarden St. Anna Advies B.V. te verstrekken aan de betreffende persoon/personen. In de overeenkomst tussen SAA en de betreffende nieuwe klant verklaart de klant deze documenten volledig te hebben doorgenomen en hiermee akkoord te gaan. SAA verwerkt de persoonsgegevens zodra de overeenkomst is ondertekend door de persoon/personen in kwestie.

Bij het sturen van een bericht via de website wordt tijdens het proces van inschrijving door middel van een hyperlink verwezen naar het Privacystatement St. Anna Advies B.V. Bij het verzenden van het bericht, gaat de zender hiermee akkoord.

3.5. Rechten van betrokkenen

3.5.1. AVG-privacyrechten

Op basis van de Algemene Verordening Gegevensbescherming, kan eenieder waarvan persoonsgegevens worden verwerkt door SAA de volgende privacyrechten uitoefenen:

- Recht op dataportabiliteit
  In de AVG (artikel 20) heet dit het 'recht om gegevens over te dragen'. Dit houdt in dat u het recht heeft om de persoonsgegevens te ontvangen die SAA van u heeft.

- Recht op vergetelheid
  Dit recht houdt in dat SAA in een aantal gevallen iemands persoonsgegevens moet wissen. U kunt, indien van toepassing, SAA vragen om uw gegevens te wissen met een beroep op uw recht op vergetelheid.

- Recht op inzage
  Aangezien u recht hebt op inzage in uw persoonsgegevens, mag u SAA vragen of er persoonsgegevens van u zijn vastgelegd en zo ja, welke. U hoeft geen reden te geven voor een inzageverzoek.

- Recht op rectificatie en aanvulling
  U heeft het recht om rectificatie van uw persoonsgegevens te vragen. Dat houdt in dat u SAA mag vragen uw persoonsgegevens te verbeteren, aan te vullen of af te schermen.

- Recht op verwerkingsbeperking
  De AVG geeft u in bepaalde situaties het recht op beperking van het gebruik van uw gegevens. In de AVG (artikel 18) staat dit recht omschreven als het 'recht op beperking van de verwerking'.

- Recht van bezwaar
  U heeft het recht om aan SAA te vragen uw persoonsgegevens niet meer te gebruiken. U kunt mogelijk om bijzondere persoonlijke redenen van het recht van bezwaar gebruikmaken.

- Recht op intrekking van toestemming
  U heeft het recht om uw toestemming voor een bepaalde verwerking in te trekken.

3.5.2. Gehoorgeving aan verzoeken

Alle verzoeken van klanten waarin rechten ten aanzien van persoonsgegevens worden ingeroepen, worden verzonden aan de FG van SAA via info@anna-advies.nl. Na een ingediend verzoek zal SAA de verzoeker laten weten dat er binnen één maand op het verzoek zal worden gereageerd. Indien het verzoek complex is, kan deze termijn met maximaal twee maanden worden verlengd. Indien dit het geval is, zal SAA dit binnen de initiële maand aan de verzoeker laten weten.

De FG zal vervolgens vaststellen welk recht precies wordt ingeroepen en verzamelt de in dat kader vereiste informatie. Op basis van deze informatie en het ingediende verzoek wordt besloten of, en zo ja, op welke wijze aan het verzoek van de verzoeker kan worden voldaan.

Voor de communicatie richting de verzoeker en het treffen van maatregelen naar aanleiding van een verzoek zullen in beginsel geen kosten in rekening worden gebracht bij de

verzoeker. Slechts in bepaalde uitzonderlijke gevallen zal SAA kosten in rekening brengen (een redelijke vergoeding in het licht van de administratieve kosten). Bijvoorbeeld wanneer verzoeker meerdere inzageverzoeken of herhaaldelijk ongegronde verzoeken indient. SAA mag in uitzonderingsgevallen ook weigeren om gevolg te geven aan het verzoek.

Indien gevolg wordt gegeven aan het verzoek van een verzoeker, dienen in bepaalde gevallen ook derde partijen op de hoogte te worden gesteld. In dergelijke gevallen kan het voor SAA noodzakelijk zijn om een verslag op te stellen. Het verslag dient dan ook de derde partijen te beschrijven die betrokken zijn bij het honoreren van een verzoek van de verzoeker. Dergelijke kennisgevingen laat SAA achterwege als dit onmogelijk blijkt of onevenredig veel inspanning vergt.

SAA heeft zodanige technische maatregelen genomen dat aan verzoeken van verzoekers kan worden voldaan. Zo kan SAA een verzoeker inzage verlenen in de gegevens die over hem/haar worden verzameld, kunnen gegevens worden verwijderd of verbeterd, kan de verwerking van gegevens tijdelijk worden gestaakt, en wordt er bij de intrekking van toestemming zorg voor gedragen dat de gegevens vanaf dat moment niet weer voor dat doel worden gebruikt.

Mocht het voorkomen dat een persoon, waarvan door SAA persoonsgegevens verwerkt, een klacht heeft met betrekking tot privacy, dan is deze persoon gewettigd om een klacht in te dienen bij de relevante privacytoezichthouder.

3.6. Derde partijen

SAA maakt voor het verwerken van sommige persoonsgegevens gebruik van derde partijen. Het gaat daarbij om partijen die louter ten behoeve van de dienstvoering van SAA gegevens verwerken (hierna: “Verwerkers”).

Met deze Verwerkers heeft SAA een verwerkersovereenkomst afgesloten waarin onder meer de mate van beveiliging van de persoonsgegevens die de Verwerkers voor SAA verwerken wordt beschreven. Ook bevat de verwerkersovereenkomst bepalingen omtrent het uitvoeren van specifieke acties bij de Verwerker ten bate van privacy en de procedure die moet worden gevolgd als van een incident omtrent persoonsgegevens sprake is.

SAA gebruikt de diensten van de volgende Verwerkers:

- Leverancier van het CRM-systeem, in het kader van het bedrijven van Customer Relationship Management (klantregistratie, opmaken van offertes/facturen, enz.).
- Aanbieder van het mysterycallsysteem, in het kader van het leveren van onze mysterycall-diensten.
- MailChimp voor het sturen van bijvoorbeeld de nieuwsbrief.
- Dropbox voor het intern delen van bestanden.
- G Suite voor het interne en externe e-mailverkeer van SAA.

Persoonsgegevens van klanten worden aan andere verwerkingsverantwoordelijken doorgegeven wanneer dat wettelijke vereist is of noodzakelijk is in het kader van dienstverlening voor klanten. Buiten deze situatie worden persoonsgegevens niet aan andere verwerkingsverantwoordelijken verstrekt zonder voorafgaande uitdrukkelijke toestemming van de klant.

3.7. Beveiliging

SAA hecht veel waarde aan de beveiliging van klantgegevens. SAA heeft daarom passende technische en organisatorische maatregelen genomen om deze persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Voor zover SAA gebruikmaakt van Verwerkers zijn met deze Verwerkers afspraken gemaakt over de te nemen technische en organisatorische maatregelen. Op grond van de risico's die de persoonsgegevens en de aard van de verwerking met zich meebrengen, wordt het gewenste beveiligingsniveau bepaald.

SAA heeft op grond van de verwerkersovereenkomst het recht de door de Verwerker getroffen maatregelen periodiek te auditen, testen, beoordelen en evalueren om zo te bepalen of de overeengekomen maatregelen worden nageleefd en of deze nog doeltreffend zijn en om deze zo nodig aan te laten passen.
SAA hanteert in aanvulling op het bovenstaande ook interne beveiligingsmaatregelen. Het gaat daarbij onder meer om de volgende maatregelen:

- Persoonsgegevens worden op een beveiligde wijze uitgewisseld.
- Persoonsgegevens worden niet op USB-sticks of andere mobiele dragers gekopieerd tenzij de persoonsgegevens versleuteld worden.
- Alleen de directeur/eigenaar van SAA (Roeland Wessels) heeft toegang tot personeelsdossiers.
- Alle laptops/pc's zijn beveiligd met verschillende wachtwoorden.
- Toegang tot het CRM-systeem is alleen mogelijk via een beveiligde VPN-verbinding op basis van twee-staps authenticatie.
- Devices als laptops en mobiele telefoons worden niet onbeheerd achtergelaten, worden versleuteld opgeslagen en in geval van verlies/diefstal wordt direct melding gemaakt bij SAA.
- Het is medewerkers niet toegestaan, zonder toestemming software te downloaden en/of om firewalls of virusscanner aan te passen of te verwijderen.
- Toegang tot het pand is alleen mogelijk met aan medewerkers verstrekte sleutels en alarmcodes.

De interne beveiligingsmaatregelen kunnen door SAA steekproefsgewijs worden gecontroleerd. Controle zal altijd zo kort en zo beperkt mogelijk uitgevoerd worden. Indien er een gerichte verdenking bestaat tegen een medewerker kan tot gerichte controle worden overgegaan. Aan de hand van de uitkomst van steekproeven kunnen door SAA disciplinaire maatregelen genomen worden.

Uitgangspunt binnen SAA is dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld. Zo vraagt SAA niet meer informatie van klanten dan noodzakelijk is voor de overeengekomen levering van producten en/of diensten. Ook bij het inschakelen van derde partijen, beoordeelt SAA of de door die derde partij aangeboden dienst aansluit bij het doel dat SAA voor ogen heeft en er niet meer persoonsgegevens worden verzameld dan daarvoor nodig is (*privacy by design en privacy by default*).

3.8. Datalekken

SAA heeft passende technische en organisatorische maatregelen genomen die tot doel hebben de kans op verlies of onrechtmatige verwerking van persoonsgegevens zo veel mogelijk te beperken. Ondanks deze maatregelen bestaat de kans dat zich toch een incident met betrekking tot persoonsgegevens voordoet.
Elk incident met betrekking tot persoonsgegevens moet worden gemeld aan de FG (Matthijs Heijstek via info@anna-advies.nl). De FG zal vervolgens in overleg met de directeur/eigenaar van SAA (Roeland Wessels) bepalen of:

- Er inderdaad sprake is van een incident dat betrekking heeft op persoonsgegevens;
- Welke maatregelen genomen moeten worden om het incident te stoppen en de gevolgen te beperken;
- Er een externe partij moet worden ingeschakeld om bij de oplossing van het incident te assisteren;
- Het incident aan de Autoriteit Persoonsgegevens moet worden gemeld. De melding aan de Autoriteit Persoonsgegevens zal vervolgens binnen 72 uur nadat SAA op de hoogte is gebracht van het incident plaatsvinden;
- Degenen op wie de persoonsgegevens betrekking hebben, moeten worden geïnformeerd over het incident;
- Welke maatregelen er genomen moeten worden om herhaling van het incident te voorkomen.

Aangezien de kans bestaat dat een Verwerker als eerste op de hoogte raakt van een (potentieel) incident, is in de Verwerkersovereenkomst afgesproken dat elke Verwerker SAA zo snel mogelijk op de hoogte stelt van een incident. Ook zijn er afspraken gemaakt over het oplossen van het incident en het verstrekken van nadere gegevens.

SAA documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

3.9. Bewaartermijnen

SAA hanteert een beleid voor het bewaren van persoonsgegevens. SAA bewaart persoonsgegevens in ieder geval voor de volledige duur van de overeenkomst en behoudt zich voor een periode van vijf jaar het recht om deze gegevens te raadplegen voor het contacteren van klanten in het kader van warme acquisitie, tenzij klanten expliciet aangeven hier grote bezwaren tegen te hebben. Persoonsgegevens die niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld en tevens niet op grond van andere wetgeving bewaard moeten worden, worden door SAA verwijderd, of op grond van de Algemene Verordening Gegevensbescherming, artikel 89, lid 1, bewaard voor historische, statistische of wetenschappelijke doeleinden, voor een periode van in ieder geval vijf jaar.

3.10. Doorgifte buiten EER

SAA slaat gegevens van klanten in beginsel niet op buiten de Europese Economische Ruimte (EER). Indien SAA persoonsgegevens toch buiten de EER opslaat, bijvoorbeeld omdat een Verwerker van SAA daar gevestigd is, draagt SAA er zorg voor dat de doorgifte

alleen plaatsvindt als de Europese Commissie heeft aangegeven dat het betreffende land een passend beschermingsniveau biedt. Er zal met deze partijen een passende verwerkersovereenkomst worden getekend.