**Privacy-management-beleid conform de AVG**
**Versie 3, 24 juni 2021, Hans Snel (manager communicatie)**

Inhoud:

## 1. Waarom privacy-management voor SDZ?

Sinds enkele jaren is in de Europese Unie de General Data Protection Regulation (GDPR) van kracht. Die is in Nederland geconcretiseerd in de Algemene Verordening Gegevensbescherming (AVG). Het doel van deze wet is tweeledig: zowel de privacybescherming van burgers binnen de EU, maar tevens de vereenvoudiging van het vrij verkeer van persoonsgegevens binnen de EU en een uniforme bescherming in de verschillende landen. Dit betekent dat organisaties aan de hand van de wet voortdurend een afweging moeten maken tussen de privacybelangen van personen en hun eigen belang als organisatie.

Er zijn vijf belangrijke redenen waarom privacy-management voor SDZ van belang is:

- Als beweging verzamelen wij persoonsgegevens van geïnteresseerden in en deelnemers aan SDZ. Het is – los van wetgeving - onze morele plicht om hiermee zorgvuldig om te gaan en de privacy van de geregistreerden te waarborgen;
- Onze beweging is een samenwerking tussen inwoners en de gemeente Zeist. Het niet zorgvuldig omgaan met persoonsgegevens kan ertoe leiden dat de gemeente imagoschade leidt;
- Ook onze eigen reputatie staat op het spel, als we onzorgvuldig met persoonsgegevens omgaan;
- Alhoewel de deskundigen het er nog niet over eens zijn of de AVG ook van toepassing is op een beweging als Samen Duurzaam Zeist, willen wij het risico niet nemen. Wetsovertredingen kunnen forse boetes opleveren;
- Juist omdat wij een beweging zijn, is er een voortdurende beweging van komende en vertrekkende mensen. Het moet voor iedereen die persoonsgegevens verwerkt, kraakhelder zijn hoe wij dat binnen SDZ doen. Dat vraagt om beleid.

## 2. Analyse van de situatie

Als er voor de rechten en vrijheden van betrokkenen een hoog risico aanwezig is, is een Privacy Impact Assessment (PIA) verplicht. Alhoewel wij op voorhand het risico niet hoog inschatten, is een analyse van de situatie gewenst om vervolgens te kunnen beoordelen wat wij willen en moeten regelen. Hieronder volgt de analyse:

### *a. Welke persoonsgegevens verzamelen wij? En wat hebben we nodig?*

*website*

Binnen de website (Mett platform) onderscheiden wij verschillende groepen gebruikers. Per gebruiker registreren we een beperkt aantal gegevens:

- **Ongeregistreerde bezoekers**: Deze groep wordt door ons dus niet geregistreerd. Zij kunnen zichzelf wel bekendmaken in een reactie op berichten op de website. Zij kunnen hier zelf kiezen voor hun eigen naam of voor een pseudoniem. Vermeld worden dus de eigen naam of pseudoniem en hun reactie.
- **Nieuwsbrief-abonnees**: hiervan registreren wij:
    - Voor- en achternaam
    - E-mailadres
- **Deelnemers aan Samen Duurzaam Zeist:** het betreft hier mensen die een account aanmaken op de website. Minimaal dienen ze de volgende gegevens in te vullen:
    - Voor- en achternaam
    - E-mailadres

Daarnaast kunnen zij er zelf voor kiezen om hun profiel te verrijken met:
    - Een profielfoto
    - Eventuele titels
    - Telefoonnummers
    - Geboortedatum
    - Geslacht
    - Huisadres
    - Naam en adres van een organisatie, namens welke ze deelnemen
    - Allerlei privacy-instellingen waarmee zij zelf bepalen wat zichtbaar is voor wie

  Slecht een heel klein deel van de deelnemers verrijkt zijn profiel.
  Van deelnemers worden automatisch ook twee extra rollen geregistreerd (zij worden hierover bij hun aanmelding geïnformeerd)
    - Rol nieuwsbrief abonnee
    - Rol interne nieuwsbrief abonnee
- **Deelnemers met aanvullende rollen en rechten op de website**: paginabeheerders, subbeheerders en de beheerder voor SDZ. Van hen wordt in aanvulling een rol geregistreerd, dat hen bepaalde extra rechten geeft op de website.

In Mett registreren we momenteel precies wat we nodig hebben om:
- Bezoekers in de gelegenheid te stellen reacties te plaatsen;
- Deelnemers in de gelegenheid stellen om zich kenbaar te maken als deelnemer, met een door henzelf gekozen en aangemaakt profiel;
- Verschillende groepen in de gelegenheid te stellen extra activiteiten op de website te ondernemen;
- Degenen die dat wensen de externe en interne nieuwsbrief te sturen.

In aanvulling op het Mett platform gebruiken we voor het versturen van nieuwsbrieven MailChimp. Omdat wij nieuwsbrieven momenteel niet personaliseren (Beste <naam>), kiezen we ervoor om in MailChimp de namen niet op te nemen en alleen e-mailadressen te registreren.

*Beeldmateriaal op de website*

Voor foto's en filmpjes waarop personen herkenbaar in beeld zijn, is toestemming van de betreffende personen nodig. Mondelinge toestemming volstaat, maar schriftelijke toestemming is veiliger. Tot nu toe hebben wij hiervoor geen beleid geformuleerd.

*Decentrale registraties*

Daarnaast worden er momenteel decentraal registraties bijgehouden binnen pijlers en werkgroepen. Deze worden gebruikt om deelnemers uit te nodigen of informatie te sturen. Enkele registraties zijn bekend, maar hiervan bestaat geen overzicht.

*Chatgroepen*

We maken gebruik van chatgroepen binnen chat-applicaties (momenteel Whatsapp). Hiervoor worden door de beheerder van de betreffende groep voornaam, achternaam en 06-nummer geregistreerd. De volgende groepen zijn in gebruik:

- SDZ Communicatie: een groep voor informatie-uitwisseling over communicatie tussen alle deelnemers met een communicatierol (beheerder is manager communicatie)
- SDZ social share: een groep van deelnemers die op uitnodiging van team communicatie berichten delen via hun eigen social media accounts (beheerder is manager communicatie)
- SDZ Activatie: een groep voor informatie-uitwisseling over activatie tussen alle deelnemers met een activatierol (beheerder is manager activatie)

*Extra nodig voor activatie*

Voor de communicatiefunctie beschikken we over de gegevens die we nodig hebben. Voor de activatiefunctie (het beïnvloeden van geïnteresseerden om incidenteel of structureel deel te nemen aan activiteiten van SDZ of om zelf nieuwe activiteiten te starten) zouden we graag extra informatie over personen willen vastleggen.

Zodra besloten wordt om extra gegevens – centraal of decentraal - te gaan vastleggen, zullen we direct ook het privacy-beleid hierop aanpassen.

***b. Wat doen we met die gegevens?***

De centraal geregistreerde gegevens gebruiken we om:
- Nieuwsbriefabonnees de nieuwsbrief toe te sturen (periodiek)
- Deelnemers aan SDZ de interne nieuwsbrief toe te sturen (periodiek)
- Rollen en rechten te controleren en desgewenst aan te passen (incidenteel)
- De contactgegevens (vooral e-mailadres) van deelnemers op te zoeken ten behoeve van 1-op-1 contact (incidenteel)

Decentrale registraties worden gebruikt om:
- Deelnemers aan pijlers of initiatieven te kunnen benaderen (via e-mail of telefoon)

De chatgroepen worden gebruikt om in kleinere groepen snel informatie uit te wisselen over actuele ontwikkelingen.

Het is de huidige beheerders van persoonsgegevens niet toegestaan om deze gegevens aan derden te verstrekken, voor welk doel dan ook.

***c. Welke systemen en bestanden onderscheiden we?***

De centrale gegevens staan in het CMS van het door **Mett** aangeboden platform. Mett slaat zijn gegevens en back-ups op op servers die in Nederland staan.

Voor het versturen van de externe en interne nieuwsbrieven wordt daarnaast gebruik gemaakt van een gratis versie van de mailapplicatie **MailChimp**. Momenteel worden nieuwe aanmeldingen voor de nieuwsbrieven periodiek handmatig geëxporteerd vanuit het Mett-platform naar MailChimp. Op korte termijn zal SDZ van MailChimp overstappen op het Nederlandse mailprogramma La Posta, omdat dit in tegenstelling tot MailChimp voldoet aan de GDPR.

Voor de chat-functie gebruiken we momenteel **Whatsapp**, een applicatie van Facebook.

Decentrale bestanden worden bijgehouden in Excel en mogelijk ook in Word.

Tot slot gebruikt de manager communicatie nog een Excelbestand waarin de namen van de paginabeheerders zijn gekoppeld aan de pagina's die zij beheren. Dit bestand bevat geen andere persoonsgegevens dan hun namen en is niet privacygevoelig. Het is opgeslagen op zijn persoonlijke computer en in zijn persoonlijke cloud-omgeving.

### *d. Wie spelen hierin welke rol?*

De centrale bestanden van website en MailChimp worden beheerd door de manager communicatie van SDZ, een door de gemeente gefinancierde zelfstandige professional. Binnen SDZ is deze manager communicatie de enige die toegang heeft tot de bestanden op het Mett-platform. Naast de manager communicatie heeft ook door deze manager ingehuurde zelfstandige professional toegang tot het bestand in MailChimp.

De decentrale bestanden zijn in beheer bij pijlercoördinatoren (nu alleen pijler 4) en kerngroep-leden van initiatieven en werkgroepen.

De Whatsappgroepen zijn in beheer bij de manager communicatie en de manager activatie, eveneens een door de gemeente gefinancierde professional.

### *e. Hoe groot zijn de risico's*

Het gaat in de basis niet om privacygevoelige informatie, enkel namen en e-mailadressen. Deelnemers kunnen ervoor kiezen om hun profiel te verrijken met meer privacygevoelige informatie, zoals woonadresgegevens, telefoonnummer en leeftijd. Zoals gemeld maken de meeste deelnemers hiervan geen gebruik.

Omdat de privacy-gevoeligheid laag is, zijn ook de risico's van verlies en misbruik relatief laag. Het volgende kan er gebeuren:

- Het platform Mett of het account van MailChimp kan worden gehackt: op dat moment kunnen persoonsgegevens worden gestolen of kunnen hackers identiteitsfraude plegen.
- Een Excel-exportbestand van de manager communicatie (nodig voor het overhevelen van e-mailadressen van Mett naar MailChimp) zou verloren kunnen gaan of in handen kunnen komen van onbevoegden. Met de manager communicatie is uitdrukkelijk afgesproken dat hij alleen persoonsgegevens download van gebruikers van het SDZ-gedeelte binnen Om Zeist.
- Een beheerder van de gemeente of van een ander project of programma kan de persoonsgegevens van deelnemers aan SDZ ongeautoriseerd gebruiken en verstrekken of verliezen.
- De telefoon van de manager communicatie of de manager activatie kan worden gestolen. Als de toegangscode wordt gekraakt, kunnen onbevoegden de telefoonnummers van een beperkt aantal deelnemers aan SDZ bemachtigen.
- De decentrale bestanden kunnen in handen komen van onbevoegden. Ook dan gaat het om de persoonsgegevens van een kleine groep deelnemers.

### *f. Wat vraagt de wet van ons?*

Alleen persoonsgegevens die worden verwerkt in huiselijk of privéverband vallen niet onder de wet. Of de gegevensverwerkingen van SDZ wel onder de wet vallen, is niet met 100% zekerheid te zeggen. Voor de zekerheid volgen wijk daarom de wet.

Conform de wet moeten wij:

- Een keuze maken op basis van welke grondslagen wij gegevensverwerkingen plegen
- Een verwerkingenregister aanleggen en bijhouden
- De rechten van betrokkenen met betrekking tot hun persoonsgegevens respecteren
- De informatie beveiligen in relatie tot de aanwezige risico's
- Voorkomende datalekken rapporteren aan de Autoriteit Persoonsgegevens
- Verwerkersovereenkomsten sluiten met organisaties die wij inschakelen voor de verwerking van persoonsgegevens
- Nieuwe systemen zo laten ontwerpen dat we daarmee de risico's op datalekken verkleinen (privacy bij design)
- Periodiek onderhoud plegen op het privacy-management

Sommige organisaties dienen daarnaast een Functionaris Gegevensbescherming (FG) te benoemen. Deze houdt toezicht op de gegevensverwerking en adviseert de verantwoordelijken. De persoon heeft goede kennis van de wetgeving, van het beleid van de organisatie en van de in gebruik zijnde systemen en gevoerde processen, maar is zelf niet verantwoordelijk voor het privacy-management. SDZ is niet verplicht om een FG aan te stellen omdat:

- SDZ geen overheidsorganisatie is
- Wij geen regelmatige, stelselmatige en grootschalige observatie plegen
- Wij geen bijzondere of strafrechtelijke gegevens verwerken

SDZ stelt geen FG aan. SDZ kan voor advies wel gebruik maken van de deskundigen binnen de gemeente Zeist heeft dit ook gedaan bij de beoordeling van dit privacy-beleid .

In de hoofdstukken hieronder worden alle genoemde onderwerpen uitgewerkt.

## 3. Keuze verwerkingsgrondslagen

De AVG kent zes grondslagen of rechtsgronden voor gegevensverwerking.

De centrale verwerkingen in Mett en MailChimp zijn nodig om de overeenkomst met nieuwsbrief-abonnees en deelnemers aan SDZ te kunnen voorbereiden en uitvoeren (grondslag 1). Immers zonder e-mailadres kunnen wij hen niet bereiken.

De decentrale verwerkingen door pijlercoördinatoren en kerngroep-leden van initiatieven en werkgroepen, zijn voor het functioneren van deze pijlers, initiatieven en werkgroepen van zodanig belang dat deze zwaarder wegen dan de belangen van de betrokkenen (grondslag 5). Dat geldt in de toekomst ook voor de gewenste gegevens ten behoeve van activatie.

De gegevensverwerking ten behoeve van Whatsapp groepen vindt plaats op basis van mondelinge of digitale toestemming van betrokkenen (grondslag 6). Betrokkenen geven toestemming om opgenomen te worden in een Whatsapp groep en kunnen hun deelname op ieder moment zelf ook weer ongedaan maken. Omdat zij zichzelf kunnen verwijderen uit de groep, houden wij geen registratie van toestemmingen bij.

Het gebruik van foto's en filmmateriaal waarop personen herkenbaar in beeld zijn, dient plaats te vinden op basis van grondslag 6, toestemming van betrokkenen. Hierop bestaat een uitzondering voor journalistieke publicaties. Hierbij hanteert de Autoriteit Persoonsgegevens de volgende criteria:

a. is de activiteit gericht op (objectieve) informatieverzameling en verstrekking?
b. gaat het om een regelmatige bezigheid?
c. gaat het erom iets van maatschappelijke strekking aan de orde te stellen?
d. kent de publicatie een recht van repliek of rectificatie achteraf?

Voor SDZ gelden alle vier de criteria. Wij hoeven dus niet vooraf toestemming te vragen aan de personen die herkenbaar in beeld zijn. Wel zullen wij zoveel mogelijk vooraf aankondigen dat mensen bezwaar kunnen maken tegen publicaties van beeldmateriaal waarop zij herkenbaar staan afgebeeld. Ook zullen wij verzoeken om beeldmateriaal te verwijderen waarop mensen herkenbaar staan afgebeeld in principe honoreren, tenzij deze personen tevoren uitdrukkelijk toestemming hebben gegeven voor publicatie en wij hiervoor kosten hebben gemaakt. In dat geval zoeken wij in overleg met de persoon in kwestie naar een goede oplossing.

## 4. Functionaris gegevensbescherming

Wij stellen geen vaste FG aan. Wel kunnen wij, zodra dat nodig is, experts van de gemeente Zeist raadplegen, onder wie iemand met de rol van FG voor de gemeente Zeist.

## 5. Verwerkingsregister

SDZ houdt een register bij van alle verwerkingen van persoonsgegevens waarvoor ze verantwoordelijk is. Dit register is opgenomen in bijlage I en zal bij wijzigingen in de structurele verwerkingen en bij nieuwe incidentele verwerkingen worden bijgewerkt. Daarnaast wordt het jaarlijks geactualiseerd, tezamen met dit beleid.

## 6. Het respecteren van de rechten van betrokkenen

De betrokkenen van wie wij persoonsgegevens verwerken hebben verschillende rechten. Hieronder geef ik aan op welke wijze wij deze rechten gaan respecteren:

*Informeren*

Op het moment dat betrokkenen zich registreren op de website, informeren wij hen over wat wij met de gegevens doen en hoe zij met ons contact kunnen opnemen. Op dit moment hanteren wij een privacyverklaring, die niet helemaal voldoet aan de eisen. Dit geldt ook voor de tekst die wij opnemen onder de nieuwsbrieven, die wij vanuit MailChimp verzenden.

In bijlage II is de tekst opgenomen van onze nieuwe privacyverklaring. Beheerders van decentrale bestanden wordt gevraagd betrokkenen ook te informeren. In bijlage II is ook een tekst opgenomen, die zij daarvoor kunnen gebruiken. Daarnaast is over decentrale bestanden ook informatie opgenomen in de privacyverklaring.

*Inzage*

Betrokkenen hebben het recht om hun persoonsgegevens in te zien. Binnen Mett hebben zij volledig toegang tot hun gegevens. Daarin is dus voorzien. Voor MailChimp en decentrale bestanden kunnen zij een verzoek doen. Wij informeren hen daarover in de nieuwe privacyverklaring.

*Verbetering*

Gegevens moeten verbeterd worden zodra betrokkenen daarom verzoeken. Dat is op dit moment al geregeld. De manager communicatie verzorgt de verbeteringen in Mett en MailChimp. In Mett kunnen deelnemers zelf ook hun gegevens verbeteren.

*Verwijdering*

Betrokkenen kunnen momenteel zelf hun account in Mett verwijderen. Zij kunnen ook zelf hun abonnement op de externe en interne nieuwsbrief ongedaan maken, via de “unsubscribe” knop onder aan de nieuwsbrief of via het sturen van een e-mail naar info@samenduurzaamzeist.nl.

Een bijzondere manier van verwijdering is het recht om vergeten te worden. Dat betekent dat de persoonsgegevens niet alleen uit het bestand zelf, maar ook uit back-ups worden verwijderd. Momenteel gebeurt dit automatisch na twee weken.

Aanvullend moeten wij:

- Periodiek binnen MailChimp alle ‘unsubscribed’ adressen verwijderen uit het bestand. Dit gaan we vanaf nu iedere maand doen.

*Overdraagbaarheid*

Betrokkenen hebben het recht om hun gegevens op zo’n manier te ontvangen dat zij kunnen worden overgedragen aan een andere dienstverlener. Omdat betrokkenen deze gegevens zelf hebben aangemaakt en kunnen inzien, heeft het verstrekken van deze gegevens dus geen meerwaarde.

*Bezwaar*

Betrokkenen mogen bezwaar maken tegen gegevensverwerkingen. Zij worden dan ook niet meer door ons geïnformeerd via nieuwsbrieven  en verliezen ook bepaalde rechten op de website. Ook dat is opgenomen in de privacyverklaring.

## 7. Informatiebeveiliging

De gegevens op de website zijn beveiligd door een door betrokkenen zelf gekozen wachtwoord. Dit wachtwoord hoeft niet periodiek te worden gewijzigd, omdat het om relatief ongevoelige data gaat. Betrokkenen kunnen er wel zelf voor kiezen om hun wachtwoord periodiek te wijzigen. Hierover zullen wij betrokkenen informeren in de privacyverklaring.

Behalve betrokkenen hebben alleen de beheerders van het platform (voor SDZ de manager communicatie) toegang tot de persoonsgegevens. Zij kunnen ook gegevens exporteren in csv-bestanden, die eenvoudig zijn op te slaan als Excel-bestand. Beheerders hebben op dit moment toegang tot niet alleen de persoonsgegevens van hun eigen project of programma, maar ook tot die van andere projecten en programma's. Dat is geen gewenste situatie, maar dit zal in de huidige versie van het platform niet worden aangepast. De beheerders krijgen van de gemeente Zeist wel de instructie om deze algemene export-functionaliteit niet te gebruiken en alleen de persoonsgegevens te downloaden van de eigen gebruikers.

Alleen de manager communicatie en een door de manager ingehuurde zelfstandige professional hebben toegang tot het MailChimp bestand. Zij delen de inloggegevens niet met anderen en deze staan ook nergens vermeld.

Decentrale bestanden worden bijgehouden door pijlercoördinatoren of kernteamleden van initiatieven of werkgroepen. In bijlage III is een veiligheidsinstructie voor hen opgenomen.
De telefoons van de manager communicatie en de manager activatie zijn beveiligd met een viercijferige toegangscode.  Daarnaast zijn de Whatsapp accounts van beide managers beveiligd met verificatie in twee stappen. Dat betekent dat iemand met een ander telefoonnummer alleen het account kan kraken, als hij de pincode weet.

## 8. Meldplicht datalekken

De wet verplicht organisaties om:

- Alle datalekken, groot en klein te registreren.
- Datalekken binnen 72 uur na het bekend worden te melden bij de Autoriteit Persoonsgegevens, tenzij het betreffende lek geen risico inhoudt voor de rechten en vrijheden van betrokkenen.

*Registratieplicht*

Vermeld moeten worden de details van het datalek, de gevolgen voor betrokkenen, de corrigerende maatregelen die zijn getroffen en of het datalek is gemeld aan de Autoriteit Persoonsgegevens. Zolang ons nog geen datalek bekend is, hoeven we nog geen registratie aan te leggen.

*Meldplicht*

Wij hanteren de volgende procedure:

1) SDZ Gegevensbeheerders (teamlid communicatie, activatiemanager en decentrale gegevensbeheerders) krijgen de instructie om een datalek direct na bekend worden, maar in ieder geval binnen één werkdag te melden aan de manager communicatie;
2) De manager communicatie registreert het datalek en overlegt met een expert binnen de gemeente Zeist over vervolgstappen;
3) De betreffende gegevensbeheerder of de manager communicatie informeert eveneens binnen één werkdag alle betrokkenen over het datalek en de mogelijke consequenties en betrekt hen bij de afweging of hier sprake is van een datalek dat risico's inhoudt voor de rechten en vrijheden van betrokkenen.
4) De manager communicatie overlegt na feedback van betrokkenen met de expert van de gemeente of een melding aan de Autoriteit Persoonsgegevens nodig is.
5) Indien gewenst wordt deze melding binnen 72 uur na bekend worden van het lek gedaan;
6) De manager communicatie, de gegevensbeheerder en de expert van de gemeente formuleren samen de corrigerende maatregelen.
7) Manager communicatie en gegevensbeheerder dragen zorg voor uitvoering van de corrigerende maatregelen en voor terugkoppeling aan betrokkenen hierover.

N.B. De hierboven genoemde gegevensbeheerder kan ook de manager communicatie zijn.

## 9. Verwerkersovereenkomst

De gemeente Zeist heeft met Mett een verwerkersovereenkomst afgesloten voor het hele platform OmZeist. Dit gemeente Zeist heeft, als beheerder van het platform, vastgesteld dat het niet nodig is om een verwerkersovereenkomst af te sluiten met de manager communicatie, als beheerder van het SDZ-deel van het platform.

Voor het beperkte risico dat vastzit aan het beheer van de Whatsappgroep van het activatieteam is een verwerkersovereenkomst een te zwaar middel. Er wordt wel een beperkt aantal afspraken gemaakt.

De manager communicatie heeft, op basis van een veroordeling door de Autoriteit Persoonsgegevens in Duitsland van een bedrijf dat MailChimp gebruikt, besloten om op korte termijn over te stappen op net Nederlandse mailprogramma La Posta. Dit mailprogramma voldoet geheel aan de AVG en gaat voorafgaand aan het gebruik ook een verwerkersovereenkomst aan met de gebruiker.

## 10. Privacy by design

Privacy by design houdt in dat systemen al zo worden vormgegeven dat de privacy beter gewaarborgd is. Een belangrijke wens is dat beheerders van projecten en programma's alleen de persoonsgegevens kunnen downloaden van betrokkenen bij het betreffende project of programma. Dat is helaas in de huidige versie van Mett niet mogelijk en moet opgelost worden door heldere afspraken te maken met de verschillende beheerders: maak geen export van het totale bestand, maar doe dit alleen van de gebruikers van jouw deelplatform.

De gemeente bevestigt dat Mett het privacy-by-design principe toepast bij aanpassing van functionaliteiten en bij updates en upgrades.

Het valt te overwegen om voor de chats van Whatsapp over te stappen op het onafhankelijke en privacy-veilige Signal. Omdat Whatsapp momenteel nog een veel grotere gebruikersgroep heeft, is daartoe nog niet besloten.

## 11. Periodiek onderhoud

Dit privacy-management-beleid zal minimaal eenmaal per jaar worden geactualiseerd door de manager communicatie, ter kennisname worden gesteld aan het regieteam en gepubliceerd op de website van SDZ.

## 12. Overzicht van te ondernemen acties

1) Verwerkingsregister aanmaken: is gebeurd, zie bijlage I
2) Privacyverklaring analyseren en aanpassen, is gebeurd, zie bijlage II
3) Veiligheidsinstructie voor pijlertrekkers en werkgroep-leden, zie bijlage III
4) Afscheid nemen van MailChimp en overstappen op La Posta
5) Privacy-management-beleid en privacy-verklaring publiceren op de website
6) Decentrale beheerders van persoonsgegevens informeren en instrueren
7) Dialoog starten over overstap van Whatsapp op Signal.
8) Periodieke activiteiten:
    a. Iedere maand het verwijderen van alle abonnees van de nieuwsbrieven van SDZ uit het MailChimp bestand en uit Mett bestand (door manager communicatie)
    b. Eenmaal per jaar actualiseren van dit privacybeleid

**Bijlage I Verwerkingsregister**
Versiedatum 24 juni 2020

*Algemene informatie*

Organisatie: Samen Duurzaam Zeist
Rechtsvorm: Geen
E-mailadres: info@samenduurzaamzeist.nl
Verantwoordelijk voor privacy-management: manager communicatie
Manager Communicatie: Hans Snel, Nectar Marketing, hans.snel@nectar-marketing.nl, 06-15014732
Functionaris Gegevensbescherming: geen (niet nodig)
Verwerkingsdoeleinden: zie privacy-management document, versie 3 van 24 juni 2021
Categorieën van betrokkenen en van persoonsgegevens: idem, zie privacy-management document
Gegevensbeveiliging: idem, zie privacy-management document

*Ontvangers van gegevens*

- Manager Communicatie (beheerder Mett en MailChimp bestand, beheerder chatgroepen): Hans Snel, voor contactgegevens zie hierboven
- Medewerker Communicatie (toegang tot MailChimpbestand): Massiel Smid, zelfstandig professional, die door Hans Snel wordt ingehuurd.
- Manager Activatie (beheerder chatgroep): Willy Douma, zelfstandig professional
- Pijlertrekkers en kernteamleden van initiatieven (bekend bij manager communicatie)
- Beheerders van andere projecten en programma's op Mett platform (bekend bij Mett team van de gemeente Zeist, te verkrijgen via manager communicatie)
- Mett, leverancier van Mett platform, waarop de website draait
- MailChimp, leverancier van mailingprogramma, waarvan wij de gratis versie gebruiken

*Doorgifte aan derde landen*

Door SDZ worden geen gegevens aan derden verstrekt. Mett slaat onze persoonsgegevens (zowel primaire database als back-ups) op op een server in Nederland. De gegevens van MailChimp worden niet in de EU opgeslagen, hetgeen de reden is om op korte termijn over te stappen op het Nederlandse mailprogramma La Posta.

*Bewaartermijnen*

SDZ bewaart op de website geen persoonsgegevens van personen die zich uitschrijven als abonnee van de nieuwsbrief of als deelnemer aan SDZ. De persoonsgegevens van mensen die zich hebben uitgeschreven zijn na twee weken ook verwijderd uit de back-ups van Mett.

Abonnees van de nieuwsbrief van SDZ kunnen via de "unsubscribe"-button onder aan iedere nieuwsbrief hun abonnement beëindigen. Abonnees van de interne nieuwsbrief van SDZ kunnen zich uitschrijven door een e-mail te sturen naar info@samenduurzaamzeist.nl. Deze verzoeken worden vóór verzending van de eerstvolgende interne nieuwsbrief gehonoreerd. Eenmaal per maand verwijderen wij de e-mailadressen van abonnees die zich hebben uitgeschreven, uit het MailChimp bestand.

*Structurele verwerkingen*

| Verwerking | Doel | Door wie | Frequentie |
|---|---|---|---|
| Back-up van Mett bestanden | Gegevensbeveiliging in geval van crash of hack | Mett | Iedere dag |
| Export uit Mett platform van alle geregistreerden | Actualiseren van abonneebestand in MailChimp | Manager Communicatie | Eenmaal per maand |
| Selectie van nieuwe abonnees uit het Excelbestand en importeren in MailChimp | Actualiseren van abonneebestand in MailChimp | Manager Communicatie | Eenmaal per maand |
| Export uit Mett platform van alle geregistreerden | Actualiseren van het bestand van ontvangers van de interne nieuwsbrief | Manager Communicatie | Steeds voorafgaand aan verzending interne nieuwsbrief. Deze verschijnt enkele malen per jaar, maar niet in een vast frequentie |
| Selectie van nieuwe deelnemers SDZ uit het Excelbestand en importeren in MailChimp | Actualiseren van het bestand van ontvangers van de interne nieuwsbrief | Manager Communicatie | Steeds voorafgaand aan verzending interne nieuwsbrief. Deze verschijnt enkele malen per jaar, maar niet in een vast frequentie |
| Verwijderen van 'unsubscribed' adressen uit het MailChimp bestand | Zorgen dat we geen persoonsgegevens bewaren die we niet meer nodig hebben. | Manager Communicatie | Iedere maand in combinatie met de verzending van de maandelijkse nieuwsbrief. |
| Verwijderen van 'unsubscribed' adressen MailChimp uit het Mett-bestand | Zorgen dat we geen persoonsgegevens bewaren die we niet meer nodig hebben. | Manager communicatie | Ieder kwartaal, in de eerste week van een nieuw kwartaal |

*Incidentele verwerkingen*

Omdat het aantal medewerkers van SDZ onder de 250 ligt, heeft SDZ geen plicht om incidentele verwerkingen vast te leggen. Dat neemt niet weg dat we grotere incidentele verwerkingen wel zullen registreren. Die hebben vanaf het moment dat wij dit privacybeleid hebben geformuleerd nog niet plaatsgevonden.

**Bijlage II Privacyverklaring SDZ voor de website**

Samen Duurzaam Zeist (SDZ) is een beweging waarin inwoners, ondernemers en de gemeente samenwerken aan acties die bijdragen aan een groen, gezond en duurzaam Zeist. Wij nemen de privacy van alle betrokkenen bij SDZ uiterst serieus. Dit komt tot uitdrukking in een privacy-beleid dat wij eenmaal per jaar bijwerken en dat je kunt downloaden vanaf de pagina Documenten. In de privacyverklaring die je nu leest, vind je hoe wij jouw wettelijke recht op privacy respecteren.

Wij houden ons aan de Algemene Verordening Gegevensbescherming (AVG). Alhoewel wij hiertoe waarschijnlijk niet verplicht zijn, doen wij dat vrijwillig omdat wij privacy heel belangrijk vinden.

In deze AVG-wet staan de rechten beschreven van personen van wie wij persoonsgegevens opslaan en verwerken. Persoonsgegevens zijn al die gegevens die informatie geven over een natuurlijke persoon, een mens dus. Het kan gaan om een e-mailadres of een telefoonnummer. Maar ook bijvoorbeeld om hobby's of interesses.

Wij maken binnen SDZ onderscheid tussen vier groepen personen. Per groep beschrijven wij hoe wij de privacy-rechten van deze groep respecteren. Ben je ontevreden over hoe wij met jouw privacy omgaan? Stuur ons dan een e-mail met jouw klacht naar info@samenduurzaamzeist.nl. Dit adres kun je ook altijd gebruiken voor vragen over ons privacy-beleid.

Vind je dat wij jouw klacht niet naar tevredenheid hebben opgelost? Dan heb je het wettelijke recht om een klacht in te dienen bij de landelijke Autoriteit Persoonsgegevens.

De vier groepen personen en hun rechten:

1. Ongeregistreerde bezoekers aan de website

Om de website te bezoeken, hoef je je niet te laten registreren. Je hoeft dus geen gebruikersnaam en wachtwoord aan te maken. Je kunt vrijwel alle pagina bezoeken. En je kunt ook reageren op nieuwsberichten, op Praat-Mee-berichten en op blogs. Je kiest dan zelf een naam. Dat mag je eigen naam zijn of een verzonnen naam (pseudoniem). Je bent zelf verantwoordelijk voor jouw reactie. Als je een bericht plaatst, verklaar je daarmee ook dat je akkoord gaat met onze huisregels. Hierin staat bijvoorbeeld dat je iedereen met respect behandelt en niet discrimineert.

Na plaatsing kun jij je eigen reactie niet meer verwijderen. Wel kun je ons verzoeken om jouw reactie weg te halen. Stuur dan een e-mail naar info@samenduurzaamzeist.nl. Wij zullen jouw reactie dan binnen 5 werkdagen verwijderen.

2. Abonnee nieuwsbrief Samen Duurzaam Zeist Actueel

Wil je onze maandelijkse nieuwsbrief ontvangen? Dan slaan wij daarvoor alleen jouw naam en e-mailadres op. Dat gebeurt op twee plaatsen, op de website en in een apart e-mailprogramma dat wij gebruiken. Dat heet MailChimp. Wij gebruiken jouw gegevens alleen voor het versturen van de nieuwsbrief. Wij hebben deze gegevens goed beveiligd en verstrekken ze nooit aan anderen.

Je kunt jezelf op ieder gewenst moment weer uitschrijven voor de nieuwsbrief. Gebruik hiervoor de knop 'unsubscribe' helemaal onder aan de nieuwsbrief. Vanaf dat moment ontvang je geen

nieuwsbrieven meer. Je naam en e-mailadres staan dan nog wel maximaal een maand in ons bestand (als “uitgeschreven”). Eenmaal per maand verwijderen wij alle namen en e-mailadressen van mensen die zich hebben afgemeld voor de nieuwsbrief. Dat doen we zowel in MailChimp als op de website. Na maximaal een maand zijn jouw naam en e-mailadres dus helemaal niet meer in onze bestanden te vinden. Als je wilt dat jouw gegevens al eerder worden verwijderd, stuur ons dan een e-mail naar info@samenduurzaamzeist.nl. We zullen jouw gegevens dan binnen 5 werkdagen verwijderen.
Je kunt dit e-mailadres ook gebruiken als je wilt dat wij jouw naam of e-mailadres aanpassen. Of als je wilt weten welke gegevens wij van jou hebben opgeslagen. Ook hiervoor nemen we maximaal vijf werkdagen de tijd.

3. Deelnemers Samen Duurzaam Zeist

Je kunt je op onze website ook als deelnemer registreren. Wij hebben daarvoor alleen jouw naam en e-mailadres nodig. Je maakt zelf een wachtwoord aan, dat bij ons niet bekend is. Vanaf dat moment heb je een account op onze website. Je kunt in dit account meer informatie over jezelf kwijt. Zoals een profielfoto, contactgegevens en wat je verder kwijt wilt. Voor het gebruik van je account is dit niet nodig.

Als je een account hebt, kun je zelf berichten plaatsen op de website, zoals een blog of een praat-mee-onderwerp. Deze kun je vervolgens zelf ook weer aanpassen of verwijderen.

Als je een account aanmaakt, ga je ook akkoord met ontvangst van de nieuwsbrief Samen Duurzaam Zeist Actueel, die eenmaal per maand verschijnt. En je gaat akkoord met ontvangst van de interne nieuwsbrief Samen Duurzaam Zeist Intern. Deze verschijnt onregelmatig. Je kunt je op ieder moment ook weer afmelden voor deze nieuwsbrieven. Hoe dat werkt, vind je onderaan iedere nieuwsbrief.

Je naam en e-mailadres staan dan nog wel maximaal een maand in ons MailChimp bestand. Eenmaal per maan verwijderen wij alle namen en e-mailadressen van mensen die zich hebben afgemeld voor beide nieuwsbrieven uit ons MailChimp bestand en eenmaal per drie maanden ook uit Mett. Na maximaal drie maanden zijn jouw naam en e-mailadres dus helemaal niet meer in onze bestanden te vinden. Als je wilt dat jouw gegevens al eerder worden verwijderd, stuur ons dan een e-mail naar info@samenduurzaamzeist.nl. We zullen jouw gegevens dan binnen 5 werkdagen verwijderen.

Jouw registratie als deelnemer op de website kun je zelf aanpassen of verwijderen. Lukt dit niet, dan kun je ons een e-mail sturen. Ook hiervoor nemen we maximaal vijf werkdagen de tijd. Twee weken na verwijdering van jouw account op de website, worden jouw persoonsgegevens automatisch ook gewist op de back-ups.

4. Actieve deelnemers aan pijlers of werkgroepen

Ben je niet alleen op de website actief, maar ook binnen één van de pijlers of werkgroepen? Dan heb je regelmatig contact met andere deelnemers aan dezelfde pijler of werkgroep. Voor de communicatie tussen leden van de pijler of werkgroep worden ook persoonsgegevens verzameld en verwerkt. Wat er precies wordt bijgehouden en hoe dit gebeurt, is per pijler en werkgroep verschillend. Als je hierover meer wilt weten, vraag dit dan aan jouw contactpersoon binnen de pijler of de werkgroep. Doe dit ook als je jouw gegevens wilt inzien, wilt wijzigen of als je gegevens wilt laten verwijderen. Ben je hierover niet tevreden? Stuur ons dan een e-mailbericht via info@samenduurzaamzeist.nl.

***Vermeldingen op de website***

Op dit moment hanteren wij op de website de volgende privacy-informatie:

1. Bij het abonneren op de nieuwsbrief:

*Elke maand op de hoogte blijven van de laatste nieuwtjes? Vul hier je gegevens in!*
*Jouw naam en e-mailadres gebruiken we alleen om de nieuwsbrief van Samen Duurzaam Zeist te verzenden. Wij gaan zorgvuldig om met jouw gegevens en zorgen ervoor dat deze niet in handen komen van onbevoegden.*

*Je kunt je op ieder moment onder aan de nieuwsbrief uitschrijven.*

Deze informatie wordt aangevuld met de volgende zin:

*Meer informatie over hoe wij rekening houden met jouw rechten vind je in onze privacyverklaring <link naar document>.*

2. Bij het aanmelden als deelnemer van SDZ:

*Welkom bij Samen Duurzaam Zeist! Na registratie kun je blogs schrijven en Praat Mee onderwerpen starten. Je gaat akkoord met het ontvangen van de nieuwsbrief Samen Duurzaam Zeist Actueel én ons bericht voor actieve deelnemers, Samen Duurzaam Zeist Intern. Je kunt je hiervoor altijd weer afmelden. Op dit platform hanteren wij ook een aantal huisregels. Als je akkoord gaat met de registratie ga je ook akkoord met de huisregels van de community.* Neem ze even door.

Ook deze verklaring wordt aangevuld met de zin:
*Meer informatie over hoe wij rekening houden met jouw rechten vind je in onze privacyverklaring <link naar document>.*

3. Op de pagina Over Samen Duurzaam Zeist

**Samen Duurzaam Zeist respecteert jouw privacy**

*Wij nemen jouw privacy heel serieus. Daarom hebben wij een privacybeleid <link> geformuleerd en een privacyverklaring <link> opgesteld. Heb je hierover een vraag of opmerking? Stuur ons een e-mail via info@samenduurzaamzeist.nl*

**Bijlage III Veiligheidsinstructie voor pijlercoördinatoren en werkgroepleden SDZ**
Versiedatum 10 augustus 2020

Samen Duurzaam Zeist is een brede beweging van mensen die individueel en samen willen bijdragen aan een groen, gezond en duurzaam Zeist. Om te kunnen samenwerken, moeten we elkaar kunnen bereiken en persoonsgegevens van elkaar opslaan. Persoonsgegevens zijn al die gegevens die iets vertellen over een persoon. Dat kan dus een e-mailadres zijn of een telefoonnummer, maar ook specifieke interesses, een foto waar je op staat of de dagen waarop je inzetbaar bent.

Om ervoor te zorgen dat organisaties zorgvuldig omgaan met de privacy van personen, is er een wet in het leven geroepen, de Algemene Verordening Gegevensbescherming (AVG). En er is een instantie die waakt over de uitvoering van deze wet en die boetes kan uitdelen als organisaties zich niet aan de wet houden, de Autoriteit Persoonsgegevens (AP). Die boetes kunnen behoorlijk oplopen. De AVG is mogelijk ook van toepassing op Samen Duurzaam Zeist. Overigens, ook als de wet niet op ons van toepassing is, moeten we privacy serieus nemen. Immers, ook dat is duurzaamheid.

Om te zorgen dat wij de privacy van onze deelnemers goed handhaven, hebben we een privacy-management-beleid opgesteld dat we jaarlijks bijwerken. En we hebben voor deelnemers ook een privacyverklaring opgesteld. Beide vind je op de website via de pagina Over Samen Duurzaam Zeist.

Als jij binnen de pijler of binnen jouw werkgroep of initiatief degene bent die gegevens bijhoudt van de andere deelnemers en van geïnteresseerden, houd je dan aan de volgende gedragsregels:

1. Zorg dat maximaal twee personen bij de gegevens kunnen.
2. Bescherm het bestand waarin de gegevens staan, met een wachtwoord.
3. Deel het bestand en het wachtwoord niet met anderen dan diegenen die bevoegd zijn om de gegevens in te zien en te verwerken.
4. Zorg ervoor dat je steeds ergens een actuele back-up van je gegevens hebt opgeslagen.
5. Sla niet meer gegevens op dan je nodig hebt om binnen de pijler of werkgroep samen te werken.
6. Verwijder regelmatig gegevens die je niet meer nodig hebt, bijvoorbeeld van deelnemers die zich hebben afgemeld.
7. Is het nodig om een deel van de gegevens ter beschikking te stellen aan één van de andere deelnemers dan de gegevensbeheerders? Verstrek die persoon dan een bestand, dat alleen die gegevens bevat en beveilig dit bestand met een ander wachtwoord. Verzoek de persoon om dit bestand na gebruik weer te verwijderen van de eigen computer, Outlook en de prullenbak.
8. Informeer deelnemers en geïnteresseerden over hoe je met hun gegevens omgaat. Zie hiervoor de tekst hieronder.
9. Behandel verzoeken van deelnemers met betrekking tot hun gegevens zorgvuldig en snel.
10. Merk je of vermoed je dat het bestand in handen is gekomen van onbevoegden? Of ben je het bestand of de computer waarop het bestand staat, kwijtgeraakt? Meld dit dat zo spoedig mogelijk, maar in ieder geval binnen 24 uur aan de manager communicatie van SDZ (via info@samenduurzaamzeist.nl).

**Tekst die decentrale beheerders van persoonsgegevens kunnen gebruiken**

Beste <naam>,

Bedankt voor jouw interesse in/deelname aan <naam pijler/werkgroep>. Om goed met elkaar te kunnen samenwerken, houden we een beperkt aantal gegevens bij van de deelnemers en geïnteresseerden. Dat zijn:

- Voor en achternaam
- E-mailadres
- <aanvullen>

Omdat we jouw privacy heel belangrijk vinden, gaan we hier zorgvuldig mee om. We gebruiken de gegevens alleen maar om goed met elkaar te kunnen samenwerken. We geven de gegevens nooit aan anderen en zorgen er ook voor dat ze niet per ongeluk in handen van anderen terecht kunnen komen. Jij hebt altijd het recht om te weten wat we precies van jou hebben opgeslagen. En je mag ook altijd verzoeken om wijzigingen aan te brengen of om jouw gegevens te verwijderen uit ons bestand. Wij zullen jouw verzoek zorgvuldig en snel opvolgen. Heb je hier vragen over? Stel ze gerust aan mij of aan info@samenduurzaamzeist.nl.