

Algemene verordening gegevensbescherming (AVG)

Ten behoeve van:
Stichting van de Sande

info@stichtingvandesande.nl
www.stichtingvandesande.nl
KvK 22045334

Versie 02, 16 mei 2018

Inhoud

1. Vooraf	1
2. Inventarisatie werkzaamheden en procedures AVG	1
3. Checklists	3
4. Concrete acties	6

1. Vooraf

De AVG is vanaf 25 mei 2018 van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt –meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

2. Inventarisatie werkzaamheden en procedures AVG

- a. Alle bestuursleden van de Stichting dienen op de hoogte te zijn van de invoering van nieuwe privacyregels. De behandeling en de verdeling van taken met betrekking tot de AVG dient aan de orde te zijn geweest in een bestuursvergadering en te zijn genotuleerd.
- b. De gegevens van de aanvragers van financiële ondersteuning (hierna: de aanvragers) worden beheerd door en zijn toegankelijk voor bestuursleden die hiervoor zijn aangewezen door het bestuur, hierna te noemen: de functionarissen. De

functionarissen zijn met naam en toenaam vermeld in een speciaal register met de titel 'AVG', hierna te noemen: het register. Dit register kan digitaal zijn. In dat geval kunnen eventuele schriftelijke rapportages worden ingescand en toegevoegd. Een back-up van het register in een cloud is verplicht.

- c. De gegevensbestanden mogen niet worden gedeeld met personen die niet in dit register zijn vermeld.
- d. Wanneer de niet als functionaris aangewezen bestuursleden toch inzicht willen hebben in de bestanden, kan dat alleen op het kantoor van de Stichting onder begeleiding van een van de functionarissen. De gegevens die worden ingezien mogen niet worden vastgelegd. Van de inzage-sessie wordt melding gemaakt in het register.
- e. Zonder de schriftelijke toestemming van de aanvrager mogen diens gegevens niet worden gepubliceerd: niet in druk, niet door middel van mondelinge overdracht en niet digitaal. NB: deze toestemming dient te worden gearchiveerd door de functionaris.
- f. Zonder de schriftelijke toestemming van de aanvrager mogen foto's waarop de aanvrager is afgebeeld niet worden gepubliceerd: niet in druk, niet door middel van mondelinge overdracht en niet digitaal. NB: deze toestemming dient te worden opgenomen in het register.
- g. De aanvragers hebben te allen tijde het recht om:
 - hun gegevens in te zien
 - hun gegevens te wijzigen
 - verwijderd te worden
 - te weten wat er met hun gegevens is gebeurd en gaat gebeuren
- h. Aanmelding van een nieuwe aanvrager kan uitsluitend op individuele basis plaatsvinden door de aanvrager of diens zaakwaarnemer. Bij de aanmelding kan de aanvrager de onder 3a opgesomde persoonsgegevens opgeven.
- i. Tevens kan de aanvrager toestemming geven aan de Stichting voor het aan hem/haar versturen van digitale informatie waarbij de standaard keuze op 'nee' is ingesteld en de aanvrager dus een actie moet ondernemen om zijn/haar toestemming te geven (bijvoorbeeld een vinkje plaatsen).
- j. De hiervoor bedoelde verplichting van actieve toestemming geldt ook voor bezoekers (aanvragers en niet-aanvragers) van de website wanneer er gebruik wordt gemaakt van cookies en voor informatie die vanuit de website kan worden gedeeld op sociale platforms zoals Facebook, Twitter, Google en Instagram.

- k. De hiervoor bedoelde verplichting van actieve toestemming geldt ook voor de aanvragers die al informatie op papier of digitaal ontvingen van de Stichting. Wanneer kan worden aangetoond dat hiervoor actieve toestemming is verleend, hoeft dat niet nóg eens te gebeuren. Wanneer dat niet kan worden aangetoond, moet er alsnog om een actieve toestemming worden gevraagd.
- l. Indien de communicatie via digitale middelen en protocollen plaatsvindt, dienen deze middelen en protocollen te zijn voorzien van een afdoende beveiliging. Deze procedure betreft de website van de Stichting, de transfer-protocollen (https) en de PC, back-up-devices, cloud-faciliteiten, laptop en/of het mobiele device (tablet, mobiele telefoon) van de functionarissen. De specificaties van de wijze waarop is beveiligd dienen te worden vastgelegd en opgenomen in het register.
- m. Eventuele back-ups van gegevensbestanden vallen onder dezelfde beveiligingsprotocollen, ongeacht of deze lokaal worden opgeslagen of in een cloud.
- n. Wanneer er een datalek aan het licht komt, dient die onmiddellijk worden geregistreerd in een register. Wanneer het gaat om een substantiële hoeveelheid persoonsgegevens of een mogelijke schade voor de betrokkenen van substantiële omvang ('ernstig'), dan dient het datalek te worden gemeld bij het Meldloket van de Autoriteit Persoonsgegevens (<https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1>). In dat geval dient ook de betrokkene te worden ingelicht. Het is aan de functionarissen om te bepalen hoe ernstig een datalek is. Registratie is te allen tijde verplicht. Voorbeelden van datalekken: het zichtbaar vermelden van persoonlijke e-mailadressen (bijvoorbeeld als CC) in een e-mail, het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger, inbraak in on- of off-line adressenbestanden en het kwijtraken of de diefstal van een gegevensdrager zoals een laptop of usb-stick.

3. Checklists

- a. *De verwerking mag alleen gebeuren voor:*
 - ✓ activiteiten die, gelet op de doelstelling van de Stichting gebruikelijk zijn;
 - ✓ andere dan de hierboven bedoelde gebruikelijke activiteiten, als die door het bestuur zijn goedgekeurd;
 - ✓ het verzenden van informatie aan de aanvragers;
 - ✓ het bekend maken van informatie over aanvrager of begunstigers en activiteiten van de Stichting na instemming van de bestuursvergadering, voor zover aanwezig, op de eigen website;

- ✓ foto's en videobeelden met of zonder geluid van activiteiten van de Stichting;
- ✓ het berekenen, vastleggen en innen van contributies en giften (inclusief het in handen van derden stellen van vorderingen);
- ✓ andere activiteiten van intern beheer;
- ✓ het behandelen van geschillen;
- ✓ het doen uitoefenen van accountantscontrole.

b. Alleen de volgende persoonsgegevens mogen worden verwerkt:

- ✓ naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens (bijvoorbeeld het e-mailadres), alsmede het bankrekeningnummer van de aanvrager of de begunstiger;
- ✓ een administratienummer, indien dat geen andere informatie bevat dan de bij het vorige punt bedoelde gegevens;
- ✓ de bij het eerste punt bedoelde gegevens van de ouders, voogden of verzorgers van minderjarige aanvragers of begunstigers;
- ✓ gegevens die betrekking hebben op de aanvraagprocedure of de begunstiging. Hieronder zijn begrepen gegevens over de aard van de aanvraagprocedure of de begunstiging (bijvoorbeeld de datum van aanvang van de aanvraagprocedure en het soort aanvraag), de functie binnen de Stichting (bijvoorbeeld de functie binnen het bestuur) en de deelname aan de activiteiten van de vereniging, de stichting of publiekrechtelijke beroepsorganisatie (bijvoorbeeld de beschikbaarheid voor activiteiten);
- ✓ gegevens voor het berekenen, vastleggen en innen van contributies en giften.

c. De persoonsgegevens mogen alleen worden verstrekt aan:

- ✓ de aanvragers of begunstigers;
- ✓ de ouders, voogden of verzorgers van minderjarige aanvragers of begunstigers;
- ✓ degenen, inclusief derden, die belast zijn met de hierboven onder 3a. opgesomde werkzaamheden, of leiding geven aan de hierboven onder a. opgesomde werkzaamheden, of noodzakelijk zijn betrokken bij de hierboven onder 3a. opgesomde werkzaamheden;
- ✓ anderen, indien: de aanvrager of de begunstiger zijn ondubbelzinnige toestemming heeft verleend voor de gegevensverwerking, of de gegevensverwerking noodzakelijk is voor de nakoming van een wettelijke plicht door de Stichting, of de gegevensverwerking noodzakelijk is vanwege een vitaal belang van de

aanvrager of de begunstiger (bijvoorbeeld een dringende medische noodzaak), of de gegevens verder worden verwerkt voor historische, statistische of wetenschappelijke doeleinden (voorwaarde hierbij is dat de Stichting ervoor zorgt dat de gegevens ook alleen voor deze specifieke doeleinden verder worden verwerkt).

d. Specifieke regels voor websites

- ✓ Gegevens op de website van de Stichting worden slechts verstrekt aan: de aanvragers of begunstigers; de ouders, voogden of verzorgers van minderjarige aanvragers of begunstigers; degenen, waaronder begrepen derden, die belast zijn met of leiding geven aan de onder 3a bedoelde activiteiten of die daarbij noodzakelijkerwijs zijn betrokken, voor zover zij daartoe door het bestuur zijn geautoriseerd.
- ✓ Het bestuur draagt zorg voor een adequate toegangsbeveiliging van de website, alsmede voor een afdoende bescherming van persoonsgegevens voor verdere verwerking door zoekmachines.
- ✓ De gegevens op de website worden onverwijld verwijderd wanneer de betrokkene of diens wettelijke vertegenwoordiger daarom verzoekt.

e. Toegestane bewaartermijn

- ✓ De persoonsgegevens moeten worden verwijderd uiterlijk twee jaar nadat de aanvraag is ingediend of nadat de begunstiger heeft aangegeven dat hij niet langer als begunstiger wil worden beschouwd. Langer bewaren van de gegevens is alleen toegestaan als de persoonsgegevens noodzakelijk zijn om te voldoen aan een wettelijke bewaarplicht.

4. Concrete acties

■ = nog doen | ■ = gedaan

a. Digitaal register aanleggen met de titel 'AVG - Stichting van de Sande' met de submapjes:

- I. Protocol
- II. Beveiliging hardware
- III. Beveiliging software
- IV. Functionarissen
- V. Datalekken
- VI. Toestemmingsregister aanvragers
- VII. Toestemmingsregister functionarissen en bestuursleden

- b. Voorlichting geven over de AVG tijdens een officiële bestuursvergadering. Dit agendapunt dient te worden genotuleerd.
- c. Tijdens deze bestuursvergadering wordt vastgesteld welke bestuursleden als (AVG-) functionaris zullen gaan functioneren.
- d. De website moet worden gecertificeerd (SSL) en is daarna alleen toegankelijk via het https-protocol.
- e. Het digitale en papieren aanvraagformulier dient te worden voorzien van een niet aangevinkt vakje waarin de aanvragers toestemming kunnen geven voor publicatie van hun organisatie op de website of gedrukte media van de Stichting.
- f. Alle bestuursleden van de Stichting waarvan de namen zijn gepubliceerd in de publicaties van de Stichting waaronder zowel de website als de papieren uitgaven worden verstaan, dienen hiervoor toestemming te hebben gegeven. Deze toestemmingsverklaringen worden opgenomen in het register.
- g. Voor bestaande digitale en papieren adresbestanden geldt dat moet worden nagegaan of er door de individuele aanvragers toestemming is gegeven om nieuwsbrieven te ontvangen. Wanneer dat zo is, is geen actie vereist, wanneer dat wel zo is, moet er gevraagd worden om toestemming.
- h. De computers, laptops, backup- en cloudfaciliteiten, tablets en mobiele telefoons (ook privé, indien van toepassing) van de functionarissen waarop de gegevensbestanden van de aanvragers worden geraadpleegd, dienen beveiligd te zijn met een wachtwoord. De wijze waarop dit is gedaan dient te worden vastgelegd in het register. Dit kan heel simpel, bijvoorbeeld: *‘PC secretaris: beveiligd met een uniek persoonlijk netwerkwachtwoord; Mobiele telefoon secretaris: beveiligd met een uniek persoonlijk wachtwoord of met vingerafdruk’*, enzovoort.
- i. Invoering gedragslijn: er worden geen gegevens van aanvragers meer verstuurd (niet digitaal, niet via de post en niet fysiek overhandigd) naar anderen dan de functionarissen.
- j. Het onderhavige document (Algemene verordening gegevensbescherming, Stichting van de Sande) wordt, gedepersonaliseerd, gepubliceerd op de website van de Stichting.