

CHECKLIST AVG VERMOGENSFONDSEN

April 2018

De Algemene Verordening Gegevensbescherming (AVG) vervangt per 25 mei 2018 de huidige privacywetgeving. De AVG bevat regels voor het (automatisch) verwerken van persoonsgegevens. Deze nieuwe Europese privacywet dwingt u als organisatie tot meer actie en maatregelen wanneer u gegevens over cliënten, personeel of andere personen vastlegt. Ook als u geen personeel in dienst heeft of slechts een paar cliënten heeft. Al bij het versturen van een offerte, factuur of een nieuwsbrief dient u rekening te houden met de wet. Organisaties zijn verplicht meer transparantie en informatie te geven over het verwerken van persoonsgegevens. Organisaties mogen alleen persoonsgegevens verwerken wanneer de AVG hiervoor een grondslag geeft.

Deze checklist beoogt slechts een hulpmiddel te zijn voor de besturen en directies van vermogensfondsen om te bepalen welke maatregelen getroffen moeten worden. Ook worden standaardteksten als hulpmiddel beschikbaar gesteld. Uiteraard blijven de besturen en directies van vermogensfondsen te allen tijde zelf verantwoordelijk voor het voldoen aan de wettelijke verplichtingen die voortvloeien uit de AVG en andere wetten. De FIN zal nimmer aansprakelijk zijn voor eventuele consequenties die voortkomen uit het gebruik van deze checklist en de aangeboden standaardteksten.

Wat is een persoonsgegeven? Dat is elke informatie die direct of indirect tot een persoon herleidbaar is. In elk geval dus naam, adres, e-mailadres (privé of zakelijk), telefoonnummer, maar ook BSN, IBAN of een profielfoto en nog meer. Wat is 'verwerken' van persoonsgegevens? Dat is onder andere het opslaan van persoonsgegevens, het aanpassen, het verwijderen, maar ook het kunnen inzien of het verliezen ervan. De persoonsgegevens moeten zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand. Een bestand is elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.

Iedere organisatie en dus ook ieder vermogensfonds verwerkt dus persoonsgegevens, al is het alleen al van uw personeel, of bestuursleden en relaties. Dus is ook op u de nieuwe wet van toepassing.

Voor midden en kleine organisaties (minder dan 250 werknemers) kunnen minder strenge regels gelden. Dit is niet het geval als structureel persoonsgegevens worden verwerkt. Vermogensfondsen verwerken in het algemeen op structurele wijze persoonsgegevens.

Voor deze checklist is o.a. gebruik gemaakt van:

- *Privacy Stappenplan, Van der Steenhoven advocaten*
- *De website van de Autoriteit Persoonsgegevens www.autoriteitpersoonsgegevens.nl*

CHECKLIST AVG VERMOGENSFONDSEN

Vraag	Antwoord	Wat moet u doen	Beschikbaar hulpmiddel
Legt u persoonsgegevens van uw bestuursleden vast?	Ja	Leg schriftelijk vast (bijvoorbeeld in notulen van het bestuur) welke informatie u vast legt en waarom naar uw mening de desbetreffende informatie noodzakelijk is. Waar wordt deze informatie bewaard en is deze voldoende beveiligd?	Standaard tekstje voor informatie aan bestuursleden. (<NAAM FONDS> legt de volgende persoonsgegevens van bestuursleden vast: < OPSOMMEN>. De persoonsgegevens worden bewaard in een afgesloten kast, waarvan <NAAM> de sleutel heeft. De gegevens worden digitaal bewaard op <INVULLEN> waarvan de beveiliging op de volgende manier geregeld is: <INVULLEN>
	Nee	Geen actie nodig. Opletten als u wel persoonsgegevens van uw bestuursleden gaat vastleggen	
Heeft uw fonds personeel in dienst (geldt ook voor zzp-ers en stagiairs)	Ja	Gegevens mogen verwerkt worden als er, onder andere, een wettelijke grondslag voor is. In alle gevallen moet de verwerking transparant zijn. In de wet zijn er verschillende grondslagen vastgesteld waarvoor gegevens verwerking is toegestaan: <ul style="list-style-type: none"> • Wanneer verwerking van de gegevens noodzakelijk is voor de voorbereiding of uitvoering van een overeenkomst waarbij de betrokkenen partij is; voor de salarisuitbetaling heeft u bijvoorbeeld de bankrekeningnummers nodig van uw personeelsleden. 	Standaard tekstje voor informatie aan medewerkers op te nemen in arbeidscontracten: Om te kunnen voldoen aan de wettelijke verplichting die volgt uit de arbeidsovereenkomst zoals bijvoorbeeld het uit kunnen voeren van de salarisbetaling, bewaart <NAAM FONDS> de volgende gegevens van de

CHECKLIST AVG VERMOGENSFONDSEN

		<ul style="list-style-type: none"> • Wanneer de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting; bijvoorbeeld de plicht tot loonaangifte en de wettelijke plicht om een kopie van het identiteitsbewijs van alle werknemers in de administratie te bewaren. • Wanneer toestemming is verleend door de betrokkene. <p>Waar wordt de personeelsinformatie bewaard en is deze voldoende beveiligd?</p>	medewerkers: NAW, BSN, IBAN en een kopie van een identiteitsbewijs. De persoonsgegevens worden bewaard in het personeelsdossier in een afgesloten kast, waarvan <NAAM> de sleutel heeft. De gegevens worden digitaal bewaard op <INVULLEN> waarvan de beveiliging op de volgende manier geregeld is: <INVULLEN>
	Nee	Geen actie nodig. Opletten als er wel personeel in dienst komt.	
Werken bij uw fonds vrijwilligers?	Ja	<p>Hebt u een overeenkomst met de vrijwilligers. Gegevens mogen verwerkt worden als er, onder andere, een wettelijke grondslag voor is. In alle gevallen moet de verwerking transparant zijn. In de wet zijn er verschillende grondslagen vastgesteld waarvoor gegevens verwerking is toegestaan:</p> <ul style="list-style-type: none"> • Wanneer verwerking van de gegevens noodzakelijk is voor de voorbereiding of uitvoering van een overeenkomst waarbij de betrokkenen partij is; voor de salarisuitbetaling heeft u bijvoorbeeld de bankrekeningnummers nodig van uw personeelsleden. • Wanneer de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting; bijvoorbeeld de plicht tot loonaangifte en de wettelijke plicht om een kopie van het identiteitsbewijs van alle werknemers in de administratie te bewaren. • Wanneer toestemming is verleend door de betrokkene. 	<p>Standaard tekstje voor informatie aan vrijwilligers op te nemen in nieuwe vrijwilligersovereenkomsten.</p> <p><NAAM FONDS> bewaart de volgende gegevens van de vrijwilliger: <OPSOMMEN>. Dit is nodig omdat <BENOEMEN>. De persoonsgegevens worden bewaard in een afgesloten kast, waarvan <NAAM> de sleutel heeft. De gegevens worden digitaal bewaard op <INVULLEN> waarvan de beveiliging op de volgende manier geregeld is: <INVULLEN></p>

CHECKLIST AVG VERMOGENSFONDSEN

		<p>Hebt u geen schriftelijke overeenkomst met de vrijwilligers? Ga na wat de noodzaak is van de gegevens die u vast legt van de vrijwilligers. Leg schriftelijk vast (bijvoorbeeld in notulen van het bestuur) waarom naar uw mening de desbetreffende informatie noodzakelijk is. Informeer de vrijwilligers over hun rechten en de wijze waarop hun gegevens worden vastgelegd.</p> <p>Waar wordt de gegevens van de vrijwilligers bewaard en is deze voldoende beveiligd?</p>	<p>Standaard basis voor een tekst in de notulen. <NAAM FONDS> sluit geen overeenkomsten met de vrijwilligers af. <NAAM FONDS> bewaart de volgende gegevens van de vrijwilliger: <OPSOMMEN>. Dit is nodig omdat <BENOEMEN>. De persoonsgegevens worden bewaard in een afgesloten kast, waarvan <NAAM> de sleutel heeft. De gegevens worden digitaal bewaard op <INVULLEN> waarvan de beveiliging op de volgende manier geregeld is: <INVULLEN></p>
	Nee	Geen actie nodig. Opletten als er wel vrijwilligers komen.	
Verstrekt uw fonds giften/leningen/donaties aan individuen?	Ja	<p>Verwerking van persoonsgegevens in het kader van de voorbereiding van een overeenkomst met een individu (bij een aanvraag) is een gerechtvaardigde grondslag.</p> <p>Verder maakt de AVG een onderscheid voor onder andere genetische en biometrische gegevens; de zogenaamde bijzondere persoonsgegevens. Deze betreffen informatie omtrent ras, godsdienst, de gezondheid van een persoon en zijn extra beschermd vanuit de wet. Volgens de AVG is het verwerken van bijzondere persoonsgegevens <u>verboden</u>, tenzij er aan een van de wettelijke voorwaarden is voldaan. Een van deze voorwaarde is dat er een uitdrukkelijke toestemming is gegeven door betrokkene. NB dit is</p>	<p>Op het aanvraagformulier kan worden opgenomen dat er gegevens worden gevraagd i.v.m. uitbetaling van een gift/lening/donatie. Daarom vragen wij van u(bijvoorbeeld NAW gegevens, IBAN-nummer).</p> <p>Voorbeeld tekst:</p> <p><optie om vinkje te zetten>. Ondergetekende verstrekt nadrukkelijk en uit vrije wil de gevraagde informatie</p>

CHECKLIST AVG VERMOGENSFONDSEN

		<p>met name voor fondsen voor individuele noden en studiefondsen relevant.</p> <p>Ga na wat de noodzaak is van de informatie die u opvraagt bij de aanvragers. Leg schriftelijk vast (bijvoorbeeld in notulen van het bestuur) waarom naar uw mening de desbetreffende informatie noodzakelijk is. Stel de bewaartermijnen vast, ook in relatie tot noodzakelijkheid.</p> <p>Voor minderjarigen, kinderen jonger dan 16 jaar, is toestemming van ouder of voogd noodzakelijk.</p> <p>Waar wordt deze informatie bewaard en is deze voldoende beveiligd?</p>	<p>aan <naam van uw fonds> i.v.m. de aangevraagde gift/lening/donatie.</p> <p>Zie verder het voorbeeld voor de besluitenlijst</p>
	Nee	Geen actie nodig. Opletten als er wel giften/leningen/donaties aan individuen gedaan gaan worden.	
Verstrekt uw fonds giften/leningen/donaties aan organisaties?	Ja	<p>De gegevens van de organisatie zelf, vallen niet onder de AVG, wel die van de contactpersoon/personen. Ook bij de voorbereiding van een overeenkomst (bij de aanvraag is er een wettelijke grondslag voor het vastleggen van deze gegevens. . .)</p> <p>Ga na wat de noodzaak is van de informatie die u opvraagt bij de aanvragers. Leg schriftelijk vast (bijvoorbeeld in notulen van het bestuur) waarom naar uw mening de desbetreffende informatie noodzakelijk is.</p> <p>Waar wordt deze informatie bewaard en is deze voldoende beveiligd?</p>	<p>Op het aanvraagformulier kan worden opgenomen dat er gegevens worden gevraagd i.v.m. uitbetaling van een gift/lening/donatie. Daarom vragen wij van u(bijvoorbeeld NAW gegevens, IBAN-nummer).</p> <p>Voorbeeld tekst:</p> <p><optie om vinkje te zetten>. Ondergetekende verstrekt nadrukkelijk en uit vrije wil de gevraagde informatie</p>

CHECKLIST AVG VERMOGENSFONDSEN

			aan <naam van uw fonds> i.v.m. de aangevraagde gift/lening/donatie. Zie verder het voorbeeld voor de besluitenlijst voor het bestuur.
	Nee	Geen actie nodig. Opletten als er wel giften/leningen/donaties aan organisaties komen.	
Heeft uw fonds een privacy beleid extern (op website)	Ja	Check of in dit privacy beleid staat welke persoonsgegevens u verwerkt, hoe deze beveiligd zijn, of deze ook aan derde partijen worden verstrekt, wat de bewaartermijnen zijn en/of hoe die bepaald worden, wat de verschillende rechten van betrokkenen zijn (diegenen van wie u de persoonsgegevens verwerkt). Ook moet de naam van uw organisatie, het adres, en de contactpersoon en telefoonnummer en e-mail adres in het beleid worden opgenomen. Als u cookies gebruikt dient u daar ook volledige informatie over te geven. Plaats het privacy beleid op uw website c.q. maak een link.	Standaard tekst voor op de website: Het bestuur van <naam fonds> heeft een privacy statement vastgesteld dat u via deze <link> kan vinden.
	Nee	Maak een privacy beleid dat voldoet aan de AVG en plaats dat op uw website.	Handige tool om u te helpen bij het opstellen van uw privacy statement is https://veiliginternetten.nl/privacyverklaring/ Standaard tekst voor op de website:

CHECKLIST AVG VERMOGENSFONDSEN

			Het bestuur van <naam fonds> heeft een privacy statement vastgesteld dat u via deze <link> kan vinden.
Heeft het bestuur van uw fonds een functionaris gegevensbescherming (FG) aangewezen?	Ja	Leg schriftelijk vast (bijvoorbeeld in notulen van het bestuur) wie die persoon is en wat zijn taken en verantwoordelijkheden zijn.	
	Nee	<p>Ga na of het nodig is een FG aan te wijzen. Bij het verwerken van bijzondere persoonsgegevens is het zeer te overwegen een FG aan te stellen ook al gebeurt het verwerken niet op grote schaal. Met name fondsen voor individuele noden is dit relevant.</p> <p>Wanneer een FG niet nodig is is het goed iemand binnen de organisatie verantwoordelijk te maken voor de handhaving van het privacy beleid (bijvoorbeeld de directeur of een van de bestuursleden). Ook is deze persoon contactpersoon voor medewerkers, betrokkenen, derden en de autoriteit persoonsgegevens in zaken over privacy binnen uw organisatie. Leg schriftelijk vast (bijvoorbeeld in notulen van het bestuur) wie die persoon is.</p>	

CHECKLIST AVG VERMOGENSFONDSEN

Heeft uw fonds een intern privacyreglement	Ja	<p>Een intern privacyreglement geeft transparante informatie aan uw medewerkers over hoe er met persoonsgegevens wordt omgegaan binnen de organisatie. Check of in dit reglement ook staat hoe u omgaat met persoonsgegevens, dat deze inzichtelijk zijn, wat de rechten van de medewerkers zijn ten aanzien van hun gegevens, hoe lang u gegevens bewaard en hoe u omgaat met het delen van gegevens. Komen in het reglement alle relevante personen voor (indien van toepassing): bestuur, medewerkers, vrijwilligers, contactpersonen, particuliere aanvragers.</p> <p>Leg schriftelijk vast (bijvoorbeeld in notulen van het bestuur) dat het bestuur bekend is met de principes van <i>privacy by design</i> en <i>privacy by default</i>.</p> <p>Leg schriftelijk een beleid vast inzake datalekken.</p> <p>Leg schriftelijk een beleid vast inzake het voldoen aan verzoeken van betrokkenen die een beroep doen op hun rechten.</p> <p>Ook is het privacyreglement geschikt om andere zaken te regelen, zoals check e-mails, gebruik mobiele telefoon en laptop, USB sticks, eventueel cameratoezicht of toegangscontrole, gebruik wachtwoorden etc.. Deze zaken hebben allemaal te maken met hoe u omgaat en wilt dat er omgegaan wordt met persoonsgegevens.</p>	Zie het voorbeeld voor de besluitenlijst voor het bestuur.
	Nee	<p>Het hebben van een duidelijk privacyreglement voor uw medewerkers is verplicht. Zie hierboven over de inhoud.</p>	Zie het voorbeeld voor de besluitenlijst voor het bestuur.

CHECKLIST AVG VERMOGENSFONDSEN

Werkt u met software leveranciers / externe dienstverleners voor bijvoorbeeld uw salarisadministratie of donatieadministratie?	Ja	<p>Stel vast dat de opdracht nemende partij handelt volgens de AVG. Leg dat schriftelijk vast. Ga na of er een verwerkingsovereenkomst is of sluit deze. Denk aan:</p> <ul style="list-style-type: none"> • Tussenpersoon • Salarisadministratie • Rentmeester • Donatieadministratie • (Externe boekhouder, afhankelijk van de aard van de opdracht) • (Accountant, afhankelijk van de aard van de opdracht) • IT beheerder • Archief • Drukker van bijvoorbeeld nieuwsbrieven • Marketing organisatie die mailings verstuurd 	Zie de informatie op het FIN Extranet
	Nee	Geen actie nodig. Opletten wanneer u wel met software leveranciers / externe dienstverleners gaat werken.	
Nieuwsbrief/ mailings etc.		Het versturen van nieuwsbrieven en mailings (digitaal) mag alleen als de ontvanger zich daar actief voor heeft aangemeld. De ontvanger moet altijd de mogelijkheid hebben om zich ook direct weer af te melden.	

CHECKLIST AVG VERMOGENSFONDSEN

Hebt u een verwerkingsregister opgesteld?	Ja	Laat het bestuur het verwerkingsregister vaststellen en spreek af hoe dit register actueel blijft.	
	Nee	<p>Het verwerkingsregister is een register dat niet hoeft te worden bijgehouden als de verwerkingsverantwoordelijke minder dan 250 personeelsleden heeft, tenzij het gaat om risicovolle verwerkingen, structurele verwerkingen of verwerkingen (ook incidenteel en risicoloos) van bijzonder of strafrechtelijke persoonsgegevens. Dit houdt in dat bijna elke organisatie een verwerkingsregister moet bijhouden. U kunt er dus vanuit gaan dat u verplicht een verwerkingsregister moet bijhouden.</p> <p>In het register moet de volgende informatie worden opgenomen:</p> <ul style="list-style-type: none"> • Naam en contactgegevens • De doeleinden van de verwerking van persoonsgegevens (waarom worden de persoonsgegevens verwerkt?) • De beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens • De categorieën van ontvangers van de persoonsgegevens en de namen, en of deze in derde landen zijn gevestigd (buiten EU en EER) of internationale organisaties • De waarborgen omtrent de passende waarborgen indien aan derde landen of aan internationale organisaties • Indien mogelijk, de beoogde bewaartermijnen of hoe de bewaartermijnen zullen worden bepaald • Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen 	Voorbeeld zal separaat beschikbaar worden gesteld.