

# KBO provincie Utrecht



Katholieke Bond van en voor Ouderen

## Protocol AVG Algemene Verordening Gegevensbescherming



***“Omzien naar elkaar”***

**Opsteller:** bestuur KBO provincie Utrecht  
**Versie:** Definitief  
**Datum:** 26 november 2018  
**KvK nummer:** 40479746

## Voorwoord

Dit jaar, 2018, start de nieuwe privacywet. Op 25 mei 2018 vervangt de AVG (Algemene Verordening Gegevensbescherming) de huidige Nederlands regelgeving omtrent privacy. Binnen de EU bestaan nu nog verschillen in privacy wetgeving, met de AVG is er straks één uniforme regelgeving voor de hele Europese Unie.

Deze nieuwe wet heeft gevolgen voor o.a. verenigingen zoals de KBO. Vanaf 25 mei 2018 moet op een vastgelegde manier omgegaan worden met privacygevoelige gegevens en moet er een Functionaris Gegevensbescherming (FG) worden aangesteld. Dit is een toezichthouder op het naleven van de AVG per afdeling.

Er zijn dus veel veranderingen, vooral over hoe je met persoonsgegevens omgaat. Indien dit niet op de juiste wijze gebeurt kan dat leiden tot sancties van de landelijke toezichthouder. Bij mogelijke datalekken (gehackte systemen) kan het bestuur persoonlijk aansprakelijk worden gesteld voor de schade. Datalekken moeten direct worden gemeld bij de bevoegde autoriteiten.

De nieuwe AVG-wet werkt andersom t.o.v. de huidige privacywetgeving. Dit betekent dat een vereniging ook vooraf moet kunnen aantonen dat de zaken op orde zijn. Gaat er iets mis in de bescherming van persoonlijke gegevens dan kan een bestuurslid persoonlijk aansprakelijk gesteld worden.

De nieuwe wet regelt de bescherming van persoonlijke gegevens die een vereniging bewaart. Het gaat hierbij niet om wat mag, maar juist om wat je verplicht bent op orde te hebben. Hoe worden gegevens bewaart, hoe en waarvoor worden gegevens gebruikt, welke gegevens worden vastgelegd en beheerd. Allemaal zaken die in een protocol (register) moeten worden vastgelegd. De opzet van zo'n protocol (register) mag een vereniging zelf bepalen.

Het 'digitale bezit' van gegevens moet goed beschermd zijn (maar ook gegevens op papier moeten uiteraard aan dezelfde eisen voldoen). Iedereen die persoonlijke gegevens opslaat, moet kunnen aantonen dat hij of zij dit op een veilige en verantwoorde manier doet. Denk bij de opgeslagen gegevens bijvoorbeeld aan de ledenadministratie, de betalingsverkeeradministratie, reis- en activiteitencommissie, websites, sociale media, adverteerders e.d.

## Inhoudsopgave

	<b>Voorwoord</b>	3
	<b>Inhoudsopgave</b>	4
<b>Artikel 1</b>	<b>Wat is verplicht</b>	5
Artikel 1.1	Doelstelling van de te beheren gegevens	5
<b>Artikel 2</b>	<b>Opgeslagen gegevens op basis van inschrijfformulieren</b>	5
Artikel 2.1	Persoonsgegevens	5
Artikel 2.2	Financiële gegevens	5
Artikel 2.3	Vernietiging gegevens	6
<b>Artikel 3</b>	<b>Documentatieplicht</b>	6
<b>Artikel 4</b>	<b>Overzicht van het digitale-systeem KBO-Leden</b>	6
Artikel 4.1	Toegang tot het systeem	6
<b>Artikel 5</b>	<b>Activiteiten</b>	6
Artikel 5.1	Bijhouden verwerking gegevens volgens AVG	6
<b>Artikel 6</b>	<b>Training</b>	7
<b>Artikel 7</b>	<b>IT -zaken</b>	7
<b>Artikel 8</b>	<b>Website</b>	7
<b>Artikel 9</b>	<b>Beeldmateriaal</b>	7
<b>Artikel 10</b>	<b>Informereren leden</b>	7
<b>Artikel 11</b>	<b>Delen met derden</b>	7
<b>Artikel 12</b>	<b>Datalekken</b>	8
<b>Artikel 13</b>	<b>Functionaris Gegevensbescherming</b>	8
<b>Artikel 14</b>	<b>Projecten</b>	8
Artikel 14.1	Belastingsservice	8
Artikel 14.2	Ouderen Adviseur (OA)	9
Artikel 14.3	Veiligheidsservice	9
Artikel 14.4	Tabletcoach	9
Artikel 14.5	Nieuwe projecten	9
<b>Artikel 15</b>	<b>Slotbepaling</b>	9

## **Artikel 1      Wat is verplicht**

1. Goed vastleggen welke persoonsgegevens de vereniging opslaat
2. Aantonen dat er zorgvuldig met de persoonsgegevens wordt omgegaan (documentatieplicht)
3. Een goed en volledig overzicht van de systemen hebben die de gegevens verwerken
4. Een goed beeld hebben van wie toegang heeft tot de systemen met (gevoelige) informatie
5. Bijhouden dat de verwerking van persoonsgegevens gaat volgens de AVG-regels
6. Medewerkers (bestuurders) trainen hoe ze intern moeten omgaan met de gegevens
7. De IT-zaken goed beveiligen. Zorgen voor goede beveiligingssoftware
8. Leden informeren over het privacy beleid binnen de vereniging
9. Denk goed na hoe eventuele persoonsgegevens worden gedeeld.

### *Artikel 1.1      Doelstelling van de te beheren gegevens*

Persoonsgegevens worden beheerd i.v.m. het kunnen besturen van de provinciale bond Utrecht, het kunnen innen van afdelingsafdrachten en het kunnen verstekken van informatie per mail en/of post c.q. informatie op de website.

Voor andere doeleinden worden de gegevens niet benut.

## **Artikel 2      Opgeslagen gegevens op basis van inschrijfformulieren**

### *Artikel 2.1      Persoonsgegevens*

KBO provincie Utrecht slaat de volgende gegevens op in Microsoft Office bestanden welke worden beheerd door de medewerker van het secretariaat, secretaris en penningmeester. Om toegang te krijgen tot de bestanden zijn gebruikersnaam en wachtwoord nodig.

Opgeslagen gegevens kunnen zijn:

- ✓ NAW-gegevens van de bestuursleden van KBO provincie Utrecht,
- ✓ NAW-gegevens van de afdelingsbestuursleden in de regio van KBO provincie Utrecht,
- ✓ NAW-gegevens van relaties van KBO provincie Utrecht,
- ✓ NAW-gegevens van de landelijke besturen van KBO-PCOB;
- ✓ NAW-gegevens van de provinciale bonden van KBO-PCOB;
- ✓ E-mailadressen van bovengenoemde personen.

Statuten van KBO provincie Utrecht en de statuten van de aangesloten afdelingen worden bewaard als hard-copy in een afgesloten kast.

### *Artikel 2.2      Financiële gegevens*

De penningmeester van KBO provincie Utrecht beheert de financiële administratie van de bond waarbij Microsoft Office bestanden worden gebruikt. Deze bestanden worden bewerkt op een server welke is voorzien van de laatste updates, viruskiller en is afgeschermd met een wachtwoord en gebruikersnaam en is toegankelijk voor bestuursleden met een account, zijnde secretaris en penningmeester en bureaumedewerker (medewerker secretariaatsbureau).

### *Artikel 2.3 Vernietiging gegevens*

Niet relevante gegevens van bestuurders worden na aftreden vernietigd, evenals gegevens van niet ter zake doende relaties.

Gegevens van leden die door het secretariaat worden doorgegeven aan de zorgverzekering i.v.m. het collectief worden na doorgifte vernietigd.

### **Artikel 3 Documentatieplicht**

Om te voldoen aan de documentatieplicht heeft KBO provincie Utrecht door middel van dit protocol de procedure vastgelegd m.b.t. het beheren van privacygevoelige gegevens.

### **Artikel 4 Overzicht van het digitale systeem KBO-Leden**

De ledenadministratie van de afdelingen wordt bijgehouden in het landelijke ledensysteem dat werkt onder de verantwoordelijkheid van de landelijke vereniging KBO-PCOB. Het systeem draait op de landelijke server en is beveiligd. De URL is een https:// security systeem.

De autorisatie van dit systeem binnen de provinciale KBO is geregeld in art. 4.1

#### *Artikel 4.1 Toegang tot het systeem*

Een bestuurder binnen KBO provincie Utrecht heeft toegang tot het KBO-ledensysteem door middel van een gebruikersnaam en een wachtwoord en is specifiek bevoegd om te mogen muteren en bevoegdheden toe te wijzen in het belang van zijn of haar functie. De medewerker van het secretariaatsbureau heeft toegang het KBO-leden systeem door middel van een gebruikersnaam en een wachtwoord. Gezien de functie van de secretariaatsmedewerker en de daarbij behorende werkzaamheden is er alleen toegang tot inzage. Muteren van de gegevens is afgeschermd.

### **Artikel 5 Activiteiten**

Voor het organiseren van activiteiten zoals: de Algemene Ledenvergadering, bijeenkomsten veiligheid, tabletcoaches, webmaster e.d. is het noodzakelijk dat de aangesloten afdelingen c.q. leden zich voor dergelijke activiteiten aanmelden. Deze aanmeldingen geschieden veelal per mail. Na het verwerken van deze aanmeldingen in Microsoft Office bestanden worden de mails verwijderd. Het werken c.q. bewerken van genoemde bestanden gebeurt op een computer welke is voorzien van de laatste update van het besturingssysteem, viruskiller en firewall en is afgeschermd met een wachtwoord en gebruikersnaam.

Na de betreffende activiteiten worden de deelnamelijsten vernietigd.

#### *Artikel 5.1 Bijhouden verwerking gegevens volgens AVG*

Nieuwe persoonsgegevens van welke aard ook, worden bijgehouden volgens de AVG-regels. Relaties in welke vorm dan ook, waarvan persoonsgegevens worden gebruikt, worden hiervan in kennis gesteld. Indien de betreffende persoon dit niet wil, worden de gegevens terstond vernietigt

met dien verstande dat betrokkene wordt geïnformeerd dat deelname aan een activiteit, waarvoor de gegevens worden gebruikt, dan niet mogelijk is. **Zie verder artikel 10.**

#### **Artikel 6      Training**

Bestuursleden van KBO provincie Utrecht worden getraind in het verwerken van privacy gevoelige persoonsgegevens door middel van een korte training. Tevens ontvangt elk nieuw bestuurslid een exemplaar van dit protocol en wordt individueel getraind.

#### **Artikel 7      IT-zaken**

Elk bestuurslid dient op zijn of haar computer te werken met de laatste update van het besturingssysteem. Tevens dient er op de computer een up-to-date viruskiller en firewall aanwezig te zijn.

Persoonsgegevens mogen niet op een tablet of mobiele telefoon worden verwerkt. Voor dergelijke werkzaamheden mag alleen een goed beveiligde computer worden gebruikt.

Dit artikel is van toepassing op alle bestuurders van KBO provincie Utrecht omdat, afhankelijk van hun portefeuille, zij mogelijk in het bezit zijn/komen van persoonsgegevens.

#### **Artikel 8      Website**

Zonder toestemming van betrokkenen mag geen privacygevoelige informatie op de website van KBO provincie Utrecht worden geplaatst zoals persoonsgegevens, foto's of andere tot een persoon te herleiden informatie.

#### **Artikel 9      Beeldmateriaal**

Beeldmateriaal (foto's en video's) mogen alleen worden gemaakt met uitdrukkelijke toestemming van de betrokkenen. Voor het plaatsen van foto's en video's op de website moet eveneens uitdrukkelijk toestemming van de betrokkenen zijn.

#### **Artikel 10     Informeren leden**

Leden (provinciale afdelingen) dienen te worden geïnformeerd dat KBO provincie Utrecht werkt volgens de AVG-regels. Dit dient te geschieden tijdens de ALV (Algemene Ledenvergadering) en met een tekst op de website.

#### **Artikel 11     Delen met derden**

KBO provincie Utrecht deelt geen persoonsgegevens met derden. Een uitzondering hierop kan zijn informatie m.b.t. de zorgverzekering Zilveren Kruis i.v.m. het collectief ter controle van het lidmaatschap KBO in combinatie met het collectief.

## Artikel 12 Datalekken

Datalekken (gehackte systemen) worden direct gemeld aan de bevoegde autoriteit(en). Op dit moment is dat het meldloket van de Autoriteit Persoonsgegevens. Datalekken worden ook gemeld bij de aandachtsfunctionaris AVG van KBO-PCOB.

Met betrekking tot datalekken zal er, zoals vastgelegd in de AVG-regels, mails worden geadresseerd volgens onderstaande methode, te weten:

**Methode 1;** Mail aan een persoon met kopie aan een derde.

In vakje **Aan** staat het mailadres van de geadresseerde, in vakje **BCC** het adres van hen die een kopie ontvangen. CC wordt niet meer gebruikt.

**Methode 2;** Mail aan meerdere personen.

In vakje **Aan** staat mailadres van verzender, in vakje **BCC** het adres van alle ontvangers. CC wordt niet meer gebruikt.

**Methode 3;** Mail aan een groep personen.

In vakje **Aan** staat mailadres van verzender, in vakje **BCC** het adres van alle ontvangers. CC wordt niet meer gebruikt.

Indien men van alle personen een antwoord verwacht, dan werkt dat niet met BCC. Men beantwoordt dan naar de verzender terwijl de verzender, indien noodzakelijk de antwoorden mailt naar de andere personen.

Het is raadzaam om in het mailgericht te vermelden bij gebruik van BCC aan welke personen het bericht is verzonden. Bijvoorbeeld "dit mailbericht is verzonden aan alle voorzitters"

Indien er sprake is van een besloten groep c.q. kring kan gewoon Aan en CC worden gebruikt, mits de geadresseerden vooraf toestemming hiervoor hebben gegeven.

## Artikel 13 Functionaris Gegevensbescherming

Gezien de grote van de organisatie en de te beheren, gewone persoonsgegevens, is het niet noodzakelijk om een Functionaris Gegevensbescherming aan te stellen. Bijzondere persoonsgegevens worden bij KBO provincie Utrecht niet vastgelegd.

## Artikel 14 Projecten

### *Artikel 14.1 Belastingservice*

KBO provincie Utrecht ziet er op toe dat de HUBA's in de provincie Utrecht werken volgens de AVG-regels. Deze maatregel zal worden opgenomen in het beleidsadviesdocument van de commissie HUBA's. Er zal op gewezen worden dat de HUBA's hun werkzaamheden dienen uit te voeren op een computer die is voorzien van de laatste updates van het besturingsstelsel en tevens zijn voorzien van een up-to-date viruskiller en firewall. Betreffende computer moet zijn voorzien van een wachtwoord en gebruikersnaam.



#### *Artikel 14.2 Ouderen Adviseur (OA)*

Met betrekking tot de Ouderen Adviseur (voorheen Vrijwillige Ouderen Adviseur ((VOA)) gelden in principe dezelfde regels als voor een HUBA. Alle vertrouwelijke informatie moet beheerd worden volgens de AVG-regels.

#### *Artikel 14.3 Veiligheidsservice*

KBO provincie Utrecht ziet er op toe dat de Veiligheidsadviseurs, werkzaam in de provincie Utrecht, werken volgens de AVG-regels. In bijeenkomsten m.b.t. veiligheid zal hier aandacht aan worden besteed. Met name checklijsten e.d. dienen na het invullen bij de betrokkenen te worden achtergelaten. Eventueel verkregen informatie, op welke gebied dan ook, moet worden vernietigd en mag niet worden gedeeld.

#### *Artikel 14.4 Tabletcoach*

KBO provincie Utrecht ziet er op toe dat de Tabletcoaches, werkzaam in de provincie Utrecht, werken volgens de AVG-regels. Tabletcoaches die leden helpen met het gebruik van een tablet met zowel het besturingssysteem iOS als Android dienen alle informatie die zij onder ogen krijgen te beschouwen als strikt vertrouwelijk en mag niet worden gedeeld met derden. Wachtwoorden en gebruikersnamen zijn eigendom van de hulpvrager. Indien tijdens de uitvoering van de werkzaamheden wordt gevraagd om een wachtwoord en gebruikersnaam, dienen ze alleen door de hulpvrager te worden ingetikt.

#### *Artikel 14.5 Nieuwe projecten*

Bij de ontwikkeling van nieuwe projecten dient altijd de vraag te worden gesteld welke eisen er worden gesteld op het gebied van de privacy, met inachtneming van het gestelde volgens de AVG-regels. Nieuwe projecten worden opgenomen in een aanhangsel bij dit protocol.

### **Artikel 15 Slotbepaling**

Elke vereniging is verantwoordelijk voor het naleven van de AVG-regels.

Website Autoriteit Persoonsgegevens <https://autoriteitpersoonsgegevens.nl>

#### **Lectuur:**

Wetteksten Rijksoverheid der Nederlanden.

Privacy statement KBO-PCOB april 2018

AVG-brochure voor afdelingen van KBO-PCOB 30 april 2018