Informatie

voor commissies van beheer en penningmeesters van de Christelijke Gereformeerde Kerken

CGK dienstenbureau

Nieuwsbrief december 2017

Deze nieuwsbrief staat ook op: www.cgk.nl/informatiebrief.

Bescherming persoonsgegevens en de kerk

Kerken en verenigingen verzamelen en gebruiken persoonsgegevens van hun leden. Denk bijvoorbeeld aan: namen, adressen, berichten van geboorte en sterven, situaties waarin voorbede wordt gevraagd. Kerken hebben deze gegevens onder meer nodig om leden op de hoogte te houden van activiteiten. Ook zijn er situaties waarin ze persoonsgegevens aan andere leden en aan niet-leden kunnen doorgeven.

Verantwoord en verstandig publiceren

Met publicaties op internet of in het kerkblad van persoonsgegevens moeten we op een verantwoorde en verstandige wijze omgaan. Want mogelijk geven we veel van de 'intimiteit' van de eigen gemeente en gemeenteleden prijs aan een potentieel groot publiek. Terwijl de informatie eigenlijk alleen bedoeld is voor een beperkte doelgroep: de eigen gemeente. Bovendien ontvangt deze doelgroep (de gemeente) het kerkblad of de overige informatie vaak ook op een andere wijze. We moeten ons dus per bericht afvragen of publicatie noodzakelijk is. Is er sprake van een toegevoegde waarde of gerechtvaardigd belang van de publicatie op de website? Kan iemand met verkeerde bedoelingen misbruik maken van de informatie die wij beschikbaar stellen?

Nieuwe regels in mei 2018

De overheid heeft in de Wet Bescherming Persoonsgegevens (WBP) regels opgesteld ter bescherming van de privacy. In deze wet staan de rechten van de persoon waarvan de persoonsgegevens gebruikt worden, en de plichten van de organisatie die de gegevens gebruikt.
Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG, ook wel GDPR) van toepassing. Deze vervangt de WBP. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU).

Meer informatie

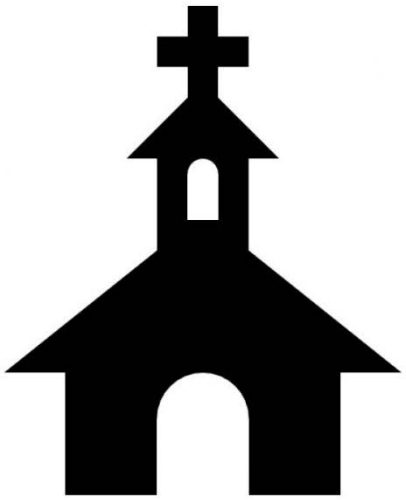
Uitgebreide informatie over de AVG (GDPR) is te vinden op:

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/de_avg_in_een_notendop.pdf

Ook in de (verouderde) handleiding WBP staat praktische informatie: www.rijksoverheid.nl/binaries/rijksoverheid/documenten/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens/handleiding-wet-bescherming-persoonsgegevens.pdf

Privacy in de kerk

De waarborging van privacy is een belangrijk onderwerp. De Autoriteit Persoonsgegevens kan voor overtreding van de WBP (per mei 2018 AVG) boetes uitdelen. Het is belangrijk om zorgvuldig om te gaan met persoonsgegevens van kerkleden.
De kerk moet daarom in eenvoudige taal precies en volledig uitleggen (in een privacyverklaring) wat zij doet met persoonlijke gegevens. Ook moet zij gebruikers/bezoekers wijzen op hun rechten, zoals het aanpassen van gegevens, inzage in dossiers of zelfs het laten vernietigen daarvan.
Vanuit de gedachte van risicobeheersing vereist de AVG dat u het minimale aan persoonsgegevens bewaart. U moet dus actief informatie weggooien wanneer deze niet meer relevant is.



Binnen eigen kerk

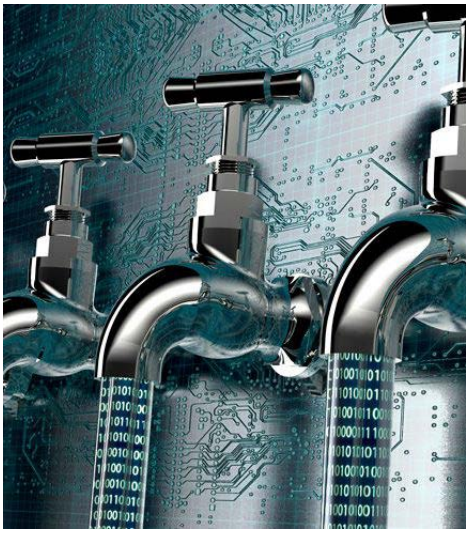
Uw kerkelijk bureau, ledenadministratie of commissie van beheer verzamelt de persoonsgegevens. Meestal in een softwaresysteem. Kerkleden kunnen individueel bezwaar aantekenen tegen registratie van persoonsgegevens binnen de eigen kerk.
Persoonsgegevens mogen doorgegeven worden aan leden binnen de eigen kerk. Denk bijvoorbeeld aan uitwisseling van adressen of relevantie informatie voor organisatoren van activiteiten in de kerk. Een afgeschermde ledenpagina op het internet is een veilige en praktische optie voor het registeren en verzamelen van noodzakelijke persoonsgegevens. In het Vrijstellingsbesluit WBP, artikel 4, vindt u welke gegevens u onder welke voorwaarden mag verzamelen als kerk.

Buiten eigen kerk

Voor het verstrekken van persoonsgegevens buiten eigen kerk is een wettelijke basis nodig. In de Wbp staat op welke gronden. De meest voorkomende grondslag is toestemming. Dat betekent dat uw persoonsgegevens alleen buiten de kerk gepubliceerd mogen worden als daarvoor expliciet toestemming is gegeven.

Gegevens en bewerkers

Daarnaast blijft de kerk verantwoordelijk voor persoonsgegevens die zij geeft aan ‘bewerkers’. Een bewerker is een persoon of organisatie aan wie de verantwoordelijke, in dit geval de kerk, gegevensverwerking heeft uitbesteed. Bijvoorbeeld het personeelsadministratiekantoor of een softwarebedrijf.
Wanneer u gebruik maakt van een softwarepakket, controleer dan of het bedrijf ISO 27001 gecertificeerd is. Dit certificaat garandeert een onafhankelijke controle op de naleving van de nieuwe privacywetgeving (bewerkersovereenkomst AVG).



Wet Meldplicht Datalekken

De wet meldplicht datalekken bepaalt dat er melding gemaakt moet worden bij inbreuk op persoonsgegevens van gevoelige aard met mogelijk ernstige gevolgen. Een inbreuk is een hack, technisch falen, verlies of diefstal van een laptop waarop persoonsgegevens van de kerk zijn opgeslagen. Persoonsgegevens van gevoelige aard gaan o.a. over betalingsgegevens, verslavingen, werk- of relatieproblemen of gegevens die kunnen worden misbruikt voor (identiteits)fraude. Een andere reden voor melding is wanneer persoonsgegevens uitlekken die media gevoelig zijn.
Volgens de huidige privacywet hoeft u alleen datalekken bij te houden wanneer u ze ook moet melden aan de toezichthouder. De nieuwe regels van de AVG stellen het verplicht alle datalekken intern te documenteren, óók datalekken die niet aan de toezichthouder gemeld hoeven te worden.
Meer informatie over wat u moet doen rond datalekken vindt u op:
http://kerkrentmeester.nl/media/verwijzingen/kerkrentmeester2017/kennisbank/organisatie/Databeheer-in-de-kerk.pdf

Dienstenbureau CGK Postbus 334, 3900 AH Veenendaal t 0318-582350 e info@cgk.nl i www.cgk.nl
IBAN NL52 INGB 0000 5353 00 t.n.v. Landelijk Kerkelijk Bureau te Veenendaal

Algemene Verordening Gegevensbescherming

Een nieuwe privacywet voor heel Europa, dat is wat de Algemene Verordening Gegevensbescherming (AVG) ons brengt. Vanaf 25 mei 2018 moet elke organisatie voldoen aan deze strenge nieuwe wet. Wat gaat er allemaal veranderen?
De AVG in negen overzichtelijke stappen:

1. Bewustwording

Zorg dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.
Let op : persoonsgegevens worden niet alleen in gedocumenteerde, gestructureerde en formele systemen vastgelegd. Ook worden kladlijstjes, geprinte wijk- of verenigingsgegevens en dergelijke bijgehouden en opgeslagen. Een zorgvuldige omgang met persoonsgegevens betekent niet alleen dat de automatiseringssystemen zijn afgeschermd; het betekent ook dat men zich bewust moet zijn van de gevoeligheid van de gegevens en de risico's die kleven aan het gebruiken van geautomatiseerde hulpmiddelen. Iedereen moet bewust zorgvuldig omgaan met gegevens en helemaal met persoonsgegevens.
Zorgvuldig gedrag kan worden bevorderd door hiervoor een aantal gedragsregels op te stellen. Gedragsregels over bijvoorbeeld het aanzetten van een slot (*lock)* op de computer als je niet op je plek zit, het hanteren van een clean desk policy, het afsluiten van kasten, niet laten slingeren van papier en dergelijke.

2. Rechten van betrokkenen

Personen krijgen recht op inzage, correctie en verwijdering van hun gegevens. Nieuw daarbij zijn:

- het *klachtrecht* van betrokkene bij de Autoriteit Persoonsgegevens (AP);
- het recht op *dataportabiliteit*:
  betrokkene heeft het recht de gegevens die een organisatie van hem/haar gebruikt op te vragen. Zo kan hij zijn gegevens bijvoorbeeld makkelijk doorgeven aan een vergelijkbare organisatie;
- het recht op *vergetelheid*
  in een aantal gevallen moeten organisaties persoonsgegevens wissen als een betrokkene hierom vraagt.

De organisatie moet tijdig kunnen reageren, vooraf bedenken hoe ze met deze rechten omgaat. Verouderde gegevens van een persoon moeten worden gewist op diens verzoek. Een verzoek van een betrokkene over zijn persoonsgegevens moet normaal binnen een maand inhoudelijk afgehandeld zijn.

3. Gegevensbewerking

De AVG stelt een *documentatieplicht* voor de verwerking van de persoonsinformatie. Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.
Onder de AVG heeft u ook een *verantwoordingsplicht*, wat inhoudt dat u kunt aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten (verwerkingsregister) is onderdeel van de verantwoordingsplicht.
U kunt het verwerkingsregister ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

4. Data Protection Impact Assesment (DPIA)

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Voor kerken zal dit in het algemeen niet spelen.

5. Gegevensbescherming door ontwerp en door standaardinstellingen

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk is voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.
Privacy by default houdt in dat u technische en organisatorische maatregelen neemt om te zorgen dat u standaard alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

6. Functionaris gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen.
Voor kerken lijkt dit niet verplicht te zijn. Wel kan het verstandig zijn om iemand de taak te geven om er op toe te zien dat de organisatie haar verplichtingen op het gebied van gegevensbescherming nakomt. Hij of zij is het eerste aanspreekpunt bij vragen over privacy en adviseert de organisatie over de toepassing van de regelgeving. Ook de bewustwording van de organisatie op het gebied van privacy, gegevensbescherming behoort tot haar/zijn taak.

7. Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren (incidentenregister). Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.

8. Bewerkersovereenkomsten

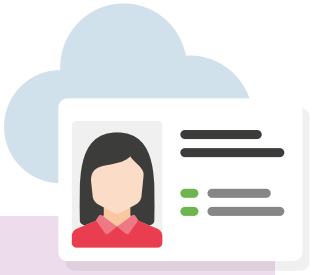
Heeft u uw gegevensverwerking uitbesteed aan een bewerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan. Belangrijke aandachtspunten zijn daarbij: goede afspraken over gebruik, over beveiliging van de gegevens, over het melden van datalekken en geheimhouding door de verwerker.

9. Toestemmingsvereisten uitgebreid

Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Privacygegevens moeten uit vrije wil, niet onder een voorwendsel of onder druk, gegeven zijn. In de toestemming moet duidelijk zijn voor welke specifieke verwerking en/of specifiek doel gegevens gebruikt worden. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan.
Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

AUTORITEIT
PERSOONSGEGEVENS

Nieuwe privacywetgeving vanaf 25 mei 2018
De AVG in een notendop



Op basis hiervan mag je persoonsgegevens verzamelen
De grondslag

- Toestemming van de gebruiker
- Vitale belangen
- Wettelijke verplichting
- Overeenkomst
- Algemeen belang
- Gerechtvaardigd belang

Het begint aan de tekentafel
Zorgvuldigheid

- Functionaris gegevens-bescherming
- Privacy by design
- Impact assessment

Technische en organisatorische maatregelen
Verplichtingen

- Register met alle verwerkingen
- Gegevens-beschermingsbeleid
- (Digitale) beveiliging

Mensen moeten controle kunnen uitoefenen
Rechten van de betrokkenen

- Recht om in te zien
- Recht om te wijzigen
- Recht om vergeten te worden
- Recht om gegevens over te dragen
- Recht op informatie

De AVG geldt vanaf 25 mei 2018

Gegevens zijn beschermd!

U heeft een goed privacyverhaal

- Voor uw doelgroep
- Voor de Autoriteit Persoonsgegevens

Aan de slag met het AVG-stappenplan!
Bereid je nu voor op de AVG

Naar het stappenplan →