Algemene Verordening Gegevensbescherming (AVG)
Toelichting, tips en stappenplan

7-5-2018

Geen uitstel meer

Op 25 mei 2018 zal de nieuwe Algemene Verordening Gegevensbescherming (AVG) in werking treden. Het Europees Parlement heeft dit al in 2016 goedgekeurd en nu wordt het ingevoerd voor de gehele Europese Unie, zelfs zonder dat er nationale wetgeving voor nodig is. Elke gemeente krijgt hiermee te maken, maar ook stichtingen, verenigingen, bedrijven en overheidsdiensten, iedereen dus. Deze nieuwe privacywetgeving van de Europese Unie vervangt de huidige Wet Bescherming Persoonsgegevens (WBP) die daarmee komt te vervallen. Er zal geen uitstel zijn, maar **laat je niet gek maken**, want de Autoriteit Persoonsgegevens (AP) zal niet bij de kerken beginnen met controleren. Wel heeft het direct gevolgen als er een datalek of een klacht binnenkomt bij de AP. Voor nu is het voldoende als men kan aantonen dat men bezig is de AVG te implementeren.

Tijd en geld en moeite

Het gaat iedereen tijd en geld en moeite kosten. Met onderstaand stappenplan heeft u een handvat voor de implementatie. De AVG heeft invloed op de manier van omgaan, registreren en bewaren van gegevens. Er zullen geautomatiseerde systemen en websites aangepast moeten worden, en er moet bekeken worden welke gegevens bewaard mogen worden en welke niet, hoe er omgegaan wordt met een mogelijk datalek, en nog veel meer. Het heeft invloed op: e-mail, telefoongebruik, dataopslag, website, sociale media, nieuwsbrieven, kerkblad, en meer.

Gebruikte afkortingen

Afkorting	volledige naam met toelichting
AP	Autoriteit Persoonsgegevens Overheidsinstelling die in Nederland belast is met toezicht op de AVG
AVG	Algemene Verordening Gegevensbescherming Door de Europese Unie ingevoerde privacywetgeving
CIO	Interkerkelijk Contact In Overheidszaken Organisatie die bij de Rijksoverheid de belangen behartigt van de kerken. Er zijn dertig landelijke kerkgenootschappen aangesloten bij CIO.
FG	Functionaris Gegevensbescherming
GDPR	General Data Protection Regulation Dit is de Engelse benaming van de AVG, die ook geregeld gebruikt wordt
MN	Missie Nederland
VWO	Verwerkersovereenkomst

Advies

Dit document is een advies, een behulpzaam voorstel, maar geen compleet overzicht. Het is toegespitst op kerken, en er zijn dingen weggelaten die meestal niet van toepassing zijn op kerken. Een zendingsorganisatie zal te maken hebben met buitenlandse personen en wellicht zijn er kantoren buiten de EU. Zulke specifieke zaken worden hier niet beschreven. De stappen in het stappenplan kunnen ook in andere volgorde doorlopen worden, maar het is wel goed om te beginnen met stap 1, 2 en 3. Heeft u vragen of wilt u reageren:
ABC-gemeenten kunnen reageren naar: kantoor@abcgemeenten.nl
UNIE-gemeenten kunnen reageren naar: info@baptisten.nl

STAPPENPLAN

Stap 1: Omarm de AVG en maak dat bekend (communicatie)

Het is goed als de hoogste leiding van de gemeente hier achter gaat staan, en de AVG omarmt. Het is voor onze eigen bescherming, dus ook al zou de overheid ons dit niet opleggen, dan nog is het goed om voorzichtig, veilig en zorgvuldig om te gaan met persoonsgegevens. De AVG spoort ons aan om er nu ernst mee te maken. Denk niet dat het zo'n vaart niet zal lopen. Het is een wettelijke verplichting om ons te houden aan de AVG.
Maak het bekend in de gemeente dat je met de AVG bezig bent. Dan zal niemand vreemd opkijken als er daarna maatregelen genomen worden. Want de invloed van de AVG reikt ver en heeft invloed op veel terreinen.
Het gaat elke gemeente tijd en geld en moeite kosten. Maak hier ruimte voor, en maak budget vrij.

- Leg uit waarom je dit doet, en **blijf herhalen**. Vertel wat je doet.
- Wees transparant in wat je als kerk doet met persoonsgegevens.
- Maak een AVG-pagina op de website, zoals er ook een ANBI-pagina is. Zet het geldende privacy statement daarop.

Stap 2: Wijs iemand aan

Maak één persoon binnen de gemeente verantwoordelijk en geef die persoon de taak om de AVG in te voeren, uiteraard in overleg met de leiding van de gemeente. Dit omvat het opstellen en uitvoeren van privacybeleid. Het is misschien wel veel werk maar je kunt dit nog zelf regelen zonder inhuur van dure experts.
De meeste kerken zijn te klein om een Functionaris Gegevensbescherming (FG) aan te stellen, maar het mag wel. Wellicht bestaat de mogelijkheid dat Missie Nederland (MN) één FG voor alle deelnemers aan MN gaat aanstellen. Dat wordt nog onderzocht. Toch is het goed om één persoon in de gemeente aan te wijzen die de implementatie gaat doen. Alle vragen komen bij die persoon terecht.

- Zorg voor mandaat en budget.
- Leg het beleid vast in een privacy statement. Gebruik daarbij geen jargon maar Jip en Janneke-taal.
- Zorg voor een goede verslaglegging naar de gemeente.
- Laat je niet gek maken, maar neem het wel serieus.
- Keep it simple, doe het stap voor stap.
- Benoem de risico's.

Stap 3: Inventariseer

Stel jezelf deze vragen:

- Op welke plaatsen worden persoonsgegevens gebruikt, bewaard, verwerkt?
- Wie heeft recht om gegevens aan te passen?
- Wie kan gegevens inzien zonder te kunnen aanpassen? Raadplegen is ook verwerken van gegevens.
- Hoe is de toegang geregeld?
- Welke maatregelen zijn nodig als de toegang beëindigd wordt?
- Welk gebruik wordt er gemaakt van de gegevens? Waarvoor registreer je bepaalde gegevens? Wat wil je ermee?
- Welke software wordt gebruikt?
- Worden er gegevens bewaard waar niets mee gedaan wordt? Kan dat weg?

- Wat hebben mensen thuis?

Denk aan: ICT, website, Excel-bestanden, clouddiensten, nieuwsbrief, e-mail, telefoon, computer, tablet, sociale media, bestanden op papier.
Let op: deze stap kost tijd.

Stap 4: Durf iets weg te gooien

Tot nog toe gingen we uit van het principe "wie bewaart die heeft wat", maar dat kan echt niet meer. Er zal nagegaan moeten worden waarom bepaalde gegevens bewaard worden, welk gebruik ervan gemaakt wordt, en wie daarbij betrokken zijn. Worden gegevens niet meer gebruikt, dan beter weggooien. Echter, er zijn ook gegevens die niet verwijderd kunnen worden, zoals een doopregister, want de doop is eenmalig en onomkeerbaar. Het kan ook zijn dat er fiscale wetgeving is om iets te bewaren. Dan gaat dat boven de AVG, en boven het recht om vergeten te worden.

- Bewaar je gegevens die niet meer gebruikt worden, dan nagaan of het weggedaan kan worden.
- Zet een papierversnipperaar neer in de gemeente en bied aan dat mensen daar hun gelezen nieuwsbrief kunnen vernietigen.
- Hoe minder gegevens, hoe beter.

Stap 5: Vraag toestemming

Het is niet meer vanzelfsprekend dat een foto geplaatst wordt. Worden er gegevens bewaard die niet meer gebruikt worden, dan kan dat weggehaald worden. Men hoeft geen toestemming te vragen indien het een gerechtvaardigd belang is om bepaalde gegevens vast te leggen.

- Omschrijf wat het gerechtvaardigd belang is en welke gegevens daar wel/niet toe behoren. Hiermee wordt bepaald wanneer toestemming gevraagd moet worden en wanneer dit niet nodig is.
- Registreer alleen wat strikt noodzakelijk is, niet meer en niet minder.
- Persoonsgegevens mogen alleen gebruikt worden voor het doel waarvoor de gegevens verstrekt zijn.
- Omschrijf hoe de toestemming ingetrokken kan worden en welke acties dan uitgevoerd worden. De AVG stelt dat dit simpel moet kunnen.
- Keep it simple: Maak een mededeling in het kerkblad dat je met AVG bezig bent, dan hoef je niet per persoon om toestemming te vragen.
- Als iemand bezwaar maakt, dan verwijder je de foto of film waarin die persoon voorkomt.
- Als er gefilmd wordt tijdens een kerkdienst, maak dan duidelijk welk deel van de zaal wel en welk deel niet in beeld zal komen.
- Als je gebruik maakt van machtigingen/incasso's, vermeld dan voor welk doel de gegevens gebruikt worden. En houd je daaraan.
- Persoonsgegevens worden niet aan derden gegeven, tenzij met uitdrukkelijke toestemming.
- Laat het privacy statement goedkeuren door de gemeentevergadering

Stap 6: Derde partijen, externen

Allemaal hebben we te maken met derde partijen die onze gegevens bewaren of bewerken, zoals een database, clouddiensten, het hosten van een website, een administratiekantoor of accountant. Het is iets nieuws van de AVG dat er een Verwerkersovereenkomst (VWO) opgesteld moet worden met elke externe partij.

- Ga zorgvuldig na welke gegevens gedeeld worden met externe partijen en voor welk doel.
- De kerk blijft verantwoordelijk voor de gegevens die gedeeld worden met externen.
- **Gebruik niet zomaar de VWO van een leverancier,** want die is er vaak op gericht de aansprakelijkheid voor de leverancier te beperken. Dan staat er bijvoorbeeld bij de voorwaarden dat een vergoeding niet hoger kan zijn dan het factuurbedrag. Trap daar niet in. Maak de leverancier medeverantwoordelijk.
- Neem zelf het initiatief naar leveranciers.
- Een VWO is voor een beperkte periode, daarna herzien, verlengen of opzeggen.
- Zorg dat je begrijpt wat in de VWO staat, ook het technisch jargon. Schakel zo nodig een deskundige in.
- Beperk het aantal leveranciers.
- Gebruik geen leveranciers van buiten de Europese Unie want die hoeven zich niet te houden aan de AVG, ook al beloven sommigen (zoals Facebook) dat wel te doen. Zoek Europese alternatieven, zoals LaPosta in plaats van MailChimp.
- Kerken werken veel met vrijwilligers. Met hen sluit je geen VWO, maar neem enkele voorwaarden op in een vrijwilligersovereenkomst.
- Medewerkers in dienst hebben een arbeidsovereenkomst. Hierin kunnen privacyvoorwaarden opgenomen worden.
- Een VWO hoef je niet af te sluiten met een bank of een pensioenfonds want die zijn zelf verwerkingsverantwoordelijk volgens AVG-regels.
- Maak geen gebruik van clouddiensten van Google (Google Drive), want Google claimt eigenaar van de gegevens te zijn.

Stap 7: Omgaan met e-mail, telefoon, sociale media, ICT

Wat tips:

- Persoonsgegevens zijn niet alleen tekstueel maar ook foto, film of geluid. Hiervoor geld de AVG ook.
- Maak regelmatig een back up.
- Zend geen e-mail aan groepen mensen maar zet de mailadressen in BCC, zodat niemand alle mailadressen ziet.
- Wees bewust van wat er mis kan gaan.
- Gebruik geen papier meer.
- Als de website gebruik maakt van cookies, dan behoort een cookie statement onderdeel te zijn van het privacy statement.
- Maak bekend welke beveiligingsprocedures er zijn.
- Iedere vorm van verlies, misbruik of diefstal van persoonsgegevens kan een datalek zijn. Bijvoorbeeld: gestolen of verloren laptop, usb-stick of telefoon, inbraak op website. Maar ook een oude computer die je wegdoet zonder de harde schijf te wissen.
- Leg vooraf vast wat moet er gebeuren bij een datalek (protocol datalekken).
- Als er een datalek opgetreden is, dan moet dit gedocumenteerd worden. Als het ernstig is, dan moet het gemeld worden bij de autoriteit (AP). Als het gevolgen heeft voor de betrokken personen dan moet het ook aan hen gemeld worden.
- Het niet melden van een ernstig datalek bij AP kan hoge boetes tot gevolg hebben.
- Melden datalek: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Stap 8: Formulieren en documenten

Zowel formulieren op papier als webformulieren zullen aangepast moeten worden aan de AVG, omdat er vermeld moet worden voor welk doel de gegevens gebruikt worden. Men geeft specifiek toestemming daarvoor. Het gaat om alle formulieren waar persoonsgegevens gevraagd worden, zoals:

- Inschrijfformulier
- Aanvraagformulier
- Machtiging / incasso

Vraag alleen gegevens die nodig zijn.

Enkele voorbeeld-documenten die je (na aanpassing) kunt gebruiken:

- Voorbeeld Privacy Statement
- Voorbeeld vrijwilligersovereenkomst
- Voorbeeld Verwerkersovereenkomst
- Voorbeeld protocol databeveiliging

Op internet zijn zulke voorbeelden te vinden. Ook staan voorbeelden op de website van ABC Gemeenten:
https://www.abcgemeenten.nl/over-abc/organisatie/privacywetgeving-avg/
Hier zijn nog meer documenten te vinden waaronder de complete wetstekst.

Hoe sta ik geregistreerd?

Een verzoek om informatie "hoe sta ik geregistreerd" moet te allen tijde gehonoreerd worden. Er moet op eenvoudige en eenduidige wijze een uitdraai van de gegevens van de betreffende persoon gegeven kunnen worden.
Dit kan men gebruiken om zich elders in te schrijven.

Recht om vergeten te worden

Mensen kunnen verzoeken om hun gegevens te verwijderen uit de administratie. Dit verzoek moet op simpele wijze gedaan kunnen worden.
Voor kerken is dit lastig, omdat bepaalde gegevens niet verloren mogen gaan. Denk hierbij bijvoorbeeld aan doopregisters. De doop is onomkeerbaar, en je wilt voorkomen dat iemand nogmaals gedoopt wordt.
Bij een verzoek om gegevens te wissen kunnen bepaalde gegevens toch bewaard blijven, maar die mogen niet meer zichtbaar zijn. Alleen enkele bevoegde personen kunnen nog inzage krijgen.

- Maak bekend welke gegevens nimmer verwijderd kunnen worden.

Kinderen

Ouders geven toestemming om hun kinderen tot 16 jaar te registreren.

Bijzondere persoonsgegevens

Gegevens over religie behoren tot de bijzondere persoonsgegevens. In principe is het niet toegestaan dit te registreren, behalve wanneer je zelf een religieuze instelling bent, want dan mag het wel. Dit is een uitzondering die expliciet in artikel 9 van de AVG genoemd wordt. Ook gegevens over doop en huwelijk behoren tot de bijzondere persoonsgegevens, waarvoor bovendien geldt dat deze gegevens niet verwijderd kunnen worden, ook als daarom verzocht wordt. De doop is immers eenmalig en

onomkeerbaar. Kerken zijn verplicht de fundamentele privacyrechten te eerbiedigen. Kerken richten zich vanuit hun roeping tot mensen aan de rand van de samenleving, want voor de barmhartige Samaritaan maakt het niet uit wie hij helpt. Ook hier moet zorgvuldig omgegaan worden met persoonsgegevens.

FAQ (vaak gestelde vragen)

vraag en antwoord
Hoe hard is de invoerdatum van 25-5-2018? Het is onwaarschijnlijk dat iedereen de AVG op tijd kan invoeren, maar er is geen uitstel. De AVG zal meteen toegepast worden, bijvoorbeeld als er een klacht binnenkomt bij de AP.
Wanneer moet een FG aangesteld worden? Bij een grote organisatie of wanneer grote hoeveelheden gegevens verwerkt worden. Op dit moment is nog onduidelijk waar precies de grens ligt.
Ben ik verplicht een datalek te melden? Nee, alleen als het ernstig is. Het moet gemeld worden bij de AP, die daarover een onderzoek zal starten. Dit kan het geval zijn bijvoorbeeld als er een USB-stick met persoonsgegevens verloren raakt of als er een hacker binnendringt in een systeem met persoonsgegevens.
Geldt de AVG alleen voor geautomatiseerde systemen? Nee, het geldt voor alle persoonsgegevens, dus ook een papieren registratie (kaartenbak), op Facebook, een website, of in een kerkblad.
Moet iedereen die reeds geregistreerd is nu opnieuw toestemming geven? Nee, het is voldoende om te melden dat u bezig bent de AVG in te voeren, en dat men kan vragen hoe men geregistreerd staat, en dat men kan verzoeken vergeten te worden.
Mogen namen en preken van gastsprekers op de website geplaatst worden? Als de website openbaar is dan zou u toestemming kunnen vragen aan de betreffende spreker. Als de preken achter een inlog staan, dan hoeft het niet, want dan is het intern voor de gemeente. Wat u ook kunt doen: meteen bij het uitnodigen van een spreker aangeven dat zijn naam en preek op de website komen, tenzij hij bezwaar maakt. Dan ligt het initiatief bij de spreker. Hetzelfde kunt u doen bij oude preken die al op de website staan. Als iemand bezwaar maakt, dan wordt het meteen weggehaald.