# Privacybeleid Petrakerk Harderwijk (1.0)

## Inleiding

In onze toenemend gedigitaliseerde maatschappij krijgt privacy steeds meer aandacht. Privacy is steeds belangrijker. De Wet bescherming persoonsgegevens (Wbp) is onlangs vervangen door de Algemene verordening gegevensbescherming (Avg) en uitgebreid met een meldplicht datalekken.

Alle reden voor de Petrakerk om het privacybeleid op te stellen.

Het gebruik van persoonsgegevens is noodzakelijk voor de processen en het omzien naar elkaar en het samen gemeentezijn bij de Petrakerk en het samen kerk zijn in de Gereformeerde kerken vrijgemaakt. Opslag en verwerking van deze persoonsgegevens dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van persoonsgegevens grote schade kan berokkenen aan leden, bezoekers en andere betrokkenen. De Kerkenraad van de Petrakerk is wettelijk verantwoordelijk voor het op een juiste manier verwerken van persoonsgegevens.

Met de maatregelen beschreven in dit beleidsdocument neemt de Petrakerk haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

## 1 Reikwijdte en doelstelling van het Privacybeleid

Het privacybeleid is van belang voor alle leden, bezoekers en andere relaties van de Petrakerk. Het heeft consequenties voor het werk van alle leden, vrijwilligers, en medewerkers die met persoonsgegevens werken. Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de Petrakerk, waaronder in ieder geval alle medewerkers, leden, bezoekers en externe relaties (inhuur systemen, materialen enz.), alsmede op andere betrokkenen waarvan de Petrakerk persoonsgegevens verwerkt.

Het privacybeleid betreft de geheel of gedeeltelijk geautomatiseerde en/of systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de Petrakerk alsmede de daaraan ten grondslag liggende (al dan niet elektronische) documenten. Eveneens is het privacybeleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Het Privacybeleid heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik en tegen verlies dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij de Petrakerk.

Het Privacybeleid geeft leden, medewerkers en andere betrokkenen inzicht in hoe privacy geregeld is door de Petrakerk. En beschrijft het hoe wij omgaan met privacy. Daarnaast helpt het bij het creëren van bewustwording over het belang en de noodzaak van het beschermen van persoonsgegevens.

Het Privacybeleid beoogt:

1. Het bieden van een kader om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgestelde norm en om de taken, bevoegdheden en verantwoordelijkheden in de kerk eenduidig te beleggen.

2. Het stellen van normen: de basis voor de beveiliging van persoonsgegevens is ISO 27001.3 Maatregelen worden genomen op basis van ISO 27002.4 ISO 27018 wordt gehanteerd als richtsnoer voor cloud services en andere outsource contracten.
3. Het nemen van verantwoordelijkheid door de Kerkenraad door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor de hele kerk.
4. Heldere implementatie van het Privacybeleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen.
5. Conform de Nederlandse en Europese wetgeving te handelen.

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van Persoonsgegevens, mede ter vermijding van risico's als gevolg van het niet werken overeenkomstig de relevante wet- en regelgeving.

## 2 Beleidsprincipes Verwerking Persoonsgegevens

Algemeen beleidsuitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden gevonden tussen het belang van de Petrakerk om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

- Een verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in de AVG.
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
- Er worden geen persoonsgegevens geregistreerd en / of registraties aangehouden die niet strikt noodzakelijk zijn.
- Bij een verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
- Iedere betrokkene heeft een wettelijk recht op inzage respectievelijk verbetering, aanvulling, verwijdering, afscherming of dataportabiliteit van de in de afzonderlijke verwerkingen hem betreffende persoonsgegevens, en heeft in bepaalde gevallen het recht van verzet.
- Wij beroepen ons op en volgen de kerkenorde.

## 3 Wet- en regelgeving

Bij de Petrakerk wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

*Algemene verordening gegevensbescherming*
De Petrakerk heeft de wettelijke vereisten (waaronder het rechtmatig en zorgvuldig verwerken van persoonsgegevens en nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking van data c.q. persoonsgegevens) geïmplementeerd door middel van het Privacybeleid.

*Archiefwet*
De Petrakerk houdt zich aan de voorschriften ten aanzien van bewaartermijnen, zoals die bijvoorbeeld in de Archiefwet zijn vastgelegd, en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d.

*Telecommunicatiewet*
De Telecommunicatiewet beschrijft onder meer aan welke regels cookies op websites dienen te voldoen.

*Auteurswet*
De Auteurswet beschrijft onder meer dat het publiceren van afbeeldingen, foto's en video's niet toegestaan is wanneer een redelijk belang van de betrokkene zich daartegen verzet. Dit wordt ook wel het portretrecht genoemd.

# 4 Rollen en verantwoordelijkheden met betrekking tot Verwerking persoonsgegevens

Om de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken is een aantal rollen en verantwoordelijkheden aan functionarissen in de Petrakerk toegewezen.

## 4.1 Overlap met informatiebeveiliging

De beheerder van de website en softwaresystemen is nauw betrokken bij de implementatie van het Privacybeleid. Het zorgvuldig omgaan met persoonsgegevens valt namelijk deels onder de algemene regels rondom Informatiebeveiliging.

## 4.2 Kerkenraad en Classis

De Kerkenraad is eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen de Petrakerk en stelt het beleid, de maatregelen en de procedures op het gebied van verwerking met dit Privacybeleid vast.

De Classis ziet toe op de goede uitvoering van het privacybeleid. De FG rapporteert per half jaar aan de Kerkenraad over de werking van het beleid.

## 4.3 Functionaris voor de gegevensbescherming

De Algemene Verordening Gegevensbescherming (Avg) verplicht de Petrakerk zelf een interne toezichthouder op de Verwerking van Persoonsgegevens aan te stellen. Deze toezichthouder wordt de Functionaris voor de Gegevensbescherming (FG) genoemd. De FG houdt binnen de Petrakerk toezicht op de toepassing en naleving van de Privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de kerk.

De FG adviseert en informeert de gehele kerk en de individuele eenheden en commissies omtrent het toepassen van de Privacywetgeving. De FG draagt zorg voor de voorlichting over verwerking van persoonsgegevens aan leden, medewerkers, kerkenraadsleden, bezoeker en overige betrokkenen.
De FG bevordert het privacybewustzijn van leden.
De FG is aanspreekpunt en vraagbaak voor degenen die vragen hebben over de bescherming van persoonsgegevens en beheert het register van meldingen van verwerkingen van persoonsgegevens.
De FG heeft de rol van procesmanager bij de afhandeling van incidenten ten aanzien van privacy-issues.

## 4.4 Kerkenraadsleden

De kerkenraadsleden zijn verantwoordelijk voor de implementatie van het Privacybeleid. Zij zijn ook verantwoordelijk voor persoonsgegevens die vanuit zijn/haar eenheid in een systeem worden ingevoerd.

## 4.5 Voorzitters van commissies

Het creëren van bewustwording en de naleving van het Privacybeleid is onderdeel van elke commissie. De voorzitter van de commissie heeft de taak om:

- ervoor te zorgen dat de commissieleden op de hoogte zijn van het privacybeleid.
- het privacybewustzijn van zijn/haar leden toereikend te laten zijn;
- toe te zien op de naleving van het Privacybeleid door zijn leden;
- periodiek het onderwerp privacy onder de aandacht te brengen in vergaderingen

# 5 Governance

## 5.1 Verdeling van verantwoordelijkheden

De kerkenraad is verantwoordelijk voor verwerkingen van de persoonsgegevens waarvan zij het doel en de middelen voor de verwerking vaststelt. Zij wordt aangemerkt als de *verantwoordelijke* in de zin van de Wet bescherming persoonsgegevens. De feitelijke verwerking van persoonsgegevens wordt echter op allerlei plekken van de Petrakerk uitgevoerd.

Privacy is *ieders verantwoordelijkheid*. Van leden, bezoekers, medewerkers, en andere betrokkenen wordt verwacht dat ze zich integer gedragen en zorgvuldig omgaan met persoonsgegevens.

## 5.2 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om bij iedereen het bewustzijn m.b.t. privacy (en security) voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en goed gedrag wordt aangemoedigd.
Verhoging van het security- en privacybewustzijn van leden is de verantwoordelijkheid van de kerkenraad, commissieleden, Functionaris gegevensbescherming

## 5.4 Controle en naleving

De FG houdt toezicht op de naleving van de privacywetgeving en het Privacybeleid, inclusief de toewijzing van verantwoordelijkheden en bewustmaking.

# 6 Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens

## 6.1 Grondslag, doelbinding en belangenafweging

Het Verwerken van Persoonsgegevens moet gebaseerd zijn op een van de wettelijke gronden zoals beschreven in artikel 8 van de Wet bescherming persoonsgegevens. De Verantwoordelijke omschrijft vooraf de doeleinden voor de Verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd.

Bij elke Verwerking wordt getoetst in hoeverre het verwerken van Persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

Bij infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren.

## 6.2 Melden en documenteren van Verwerkingen

Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens dient gemeld te worden bij de FG van de Petrakerk. De FG beoordeelt de rechtsgeldigheid van de registratie en draagt zorg voor adequate documentatie.

De Verwerkingen worden voldoende gedocumenteerd (Bijlage 2) en gepubliceerd op voor de betrokkenen toegankelijke media met vermelding van het doel van de registratieregistraties en de verantwoordelijken.

## 6.3 De organisatie van de beveiliging

De Petrakerk draagt zorg voor een adequaat beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen.

## 6.4 Geheimhouding

Bij de Petrakerk worden alle Persoonsgegevens als vertrouwelijk geclassificeerd. Een ieder behoort de vertrouwelijkheid van Persoonsgegevens te kennen en daarnaar te handelen.
Ook personen voor wie niet reeds uit hoofde van ambt, commissielid of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

## 6.5 Bewaartermijnen/ vernietigingstermijnen per soort gegeven

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is, voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Persoonsgegevens dienen na het verlopen van de bewaartermijn buiten het bereik van de actieve administratie gebracht te worden. De Petrakerk zal de persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de persoonsgegevens bestemd zijn voor historische of statistische doeleinden, in een archief bewaren.

Bewaartermijnen (Bijlage 11) kunnen wettelijk zijn bepaald, zoals bij financiële gegevens, maar kunnen ook zijn vastgelegd door de Petrakerk, b.v. in een overeenkomst tussen de Petrakerk en de Betrokkenen.

## 6.6 Bijzondere Persoonsgegevens

Het verwerken van bijzondere Persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de Betrokkene of een zwaarwegend algemeen belang. Tevens gelden zwaardere eisen voor de beveiliging van deze Persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.
Onder bijzondere Persoonsgegevens vallen gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele geaardheid, strafrechtelijke gegevens en BSN.
**Een attestatie zal dus persoonlijk worden overhandigd aan het vertrekkende lid en deze zal hem persoonlijk afgeven in de nieuwe gemeente. Gegevens worden niet meer verzonden.**

## 6.7 Doorgifte Persoonsgegevens aan Derden - Uitbesteden van Verwerking aan een Bewerker

Indien de Petrakerk Persoonsgegevens laat verwerken door een *Bewerker*, wordt de uitvoering van Verwerkingen geregeld in een schriftelijke overeenkomst tussen de Petrakerk, de Verantwoordelijke, en de Bewerker.

### 6.7.1 Doorgifte Persoonsgegevens binnen de Europese Unie

De Petrakerk verstrekt Persoonsgegevens alleen aan Derden, als deze doorgifte is gebaseerd op een wettelijke grondslag.
Met betrekking tot bijzondere persoonsgegevens worden deze niet aan derden verstrekt zonder expliciete toestemming van de betrokkene.

### 6.7.2 Doorgifte Persoonsgegevens buiten de Europese Unie (inclusief de EEA)

De Petrakerk verstrekt Persoonsgegevens alleen aan Derden die zich bevinden in een land buiten de Europese Unie indien dat land in zijn geheel of de kerk specifiek een *passend beschermingsniveau waarborgt*. Voor landen met een passend beschermingsniveau hanteert de Petrakerk de lijst van landen gepubliceerd door de Europese Commissie.

De Petrakerk verstrekt Persoonsgegevens alleen aan landen zonder passend beschermingsniveau op basis van een wettelijke uitzondering zoals genoemd in artikel 77 van de Wbp. Eén van die uitzonderingen is “ondubbelzinnige toestemming”: degene van wie Persoonsgegevens doorgegeven wordt, heeft ondubbelzinnige toestemming gegeven. Een andere wettelijke uitzondering is doorgifte op basis van een modelcontract (zoals opgesteld door de Europese Commissie). Bij wijzigingen van of aanvullingen op het modelcontract is een vergunning van de minister van Veiligheid en Justitie vereist. In alle gevallen is bij doorgifte van Persoonsgegevens aan een land buiten de Europese Unie een melding bij de AP verplicht.

### 6.7.3 Derden aan wie de Petrakerk Persoonsgegevens doorgeeft (niet limitatieve lijst)

Zusterkerken,……

## 7 Incidenten met betrekking tot Persoonsgegevens

Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van incidenten of het vermoeden van incidenten in de reguliere gang van zaken en in bijzondere omstandigheden.

Iedere klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen de Petrakerk is een privacy incident. De bekendste vorm van zo’n incident is een datalek.

Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we van een datalek.

## 7.1 Melding en registratie

Leden van de Petrakerk zijn verplicht om een (vermoedelijk) ‘datalek’ en andere privacy incidenten direct te melden. Incidenten worden vanwege de efficiency bij voorkeur gemeld bij scriba@petrakerkharderwijk.nl.

Van elk incident en de afhandeling daarvan wordt door de FG een registratie bijgehouden.

Meldingen worden vertrouwelijk behandeld. De melder kan er op vertrouwen dat het doen van een melding geen persoonlijke consequenties heeft voor de melder. Een melder dient zolang het incident nog niet is afgehandeld vertrouwelijk met de melding om te gaan en hierover niet te communiceren met betrokkenen of anderen.

## 7.2 Afhandeling

De afhandeling van incidenten heeft als doel het probleem op te lossen, de schade te beperken en de wetgeving na te leven. Normaliter is de ISO in samenspraak met de FG degene die beoordeelt of er waarschijnlijk sprake is van een datalek. In dat geval worden in ieder geval de FG en de ISO betrokken in de verdere afhandeling.

De FG is verantwoordelijk voor de afhandeling van privacy incidenten.

Als het incident een datalek betreft dan wordt conform de regels van de Autoriteit Persoonsgegevens (AP) bepaald of melding aan de AP verplicht is. De melding wordt afgestemd met het Raad van Bestuur. Een melding aan de AP dient onverwijld binnen 72 uur na constatering plaats te vinden.

Wanneer het informeren van betrokkenen verplicht is conform de regels van de AP of anderszins gewenst is, wordt de communicatie in samenspraak met Communicatie verzorgd. De melder wordt geïnformeerd over de afhandeling van het incident.

# 8. Maatregelen

Richtlijnen voor kerkelijk bureau

1. Kerkelijk bureau is in staat om gegevens te anonimiseren indien gewenst door betrokkenen
2. Kerkelijk bureau heeft de mogelijkheid om bepaalde gegevens te wissen, danwel te zorgen dat deze niet in het handboek worden ingevuld/afgedrukt.
3. Aan nieuwe leden wordt meegedeeld dat hun gegevens zullen worden opgenomen in het kerkblad en het handboek tenzij zij hier schriftelijk bezwaar tegen hebben gemaakt.
4. Aan vertrekkende leden zal worden meegedeeld dat tijdens de eredienst in de mededelingen hun vertrek wordt genoemd en hun vertrek al worden gemeld in het kerkblad, inclusief hun nieuwe adres en nieuwe kerkelijke gemeente tenzij hier bezwaar tegen hebben.
   Tevens wordt aan vertrekkende leden gemeld dat hun gegevens bewaard worden in de kerkelijke administratie, tenzij zij hier bezwaar tegen hebben. Dan worden gegevens geanonimiseerd.
5. Het kerkelijk bureau communiceert aan kerkblad redactie, websitebeheerder de leden die de kerk hebben verlaten??? Waarom???? Opnemen of verwijderen???
6. Het kerkelijk bureau zorgt dat papieren versies van het handboek achter slot en grendel worden bewaard.

Richtlijnen voor een ieder die directe toegang heeft tot de ledenadministratie

7. De financiële administratie en het kerkelijk bureau worden geacht de toegang tot de gegevens op de computer waarop zij de ledenadministratie bijhouden te beveiligen tegen ongeoorloofde toegang. En voorzien van softwarebeveiliging en antivirusprogramma.

Richtlijnen voor de websitebeheerder en facebookpagina

8. Website beheerder zorgt dat alleen eigen leden, of personen direct gelieerd aan onze gemeente, toegang hebben tot het Intranet van de kerk.
9. Website beheerder zorgt dat, indien er foto's worden geplaatst op de website, waarop personen duidelijk herkenbaar zijn, deze personen hiervoor schriftelijk toestemming hebben verleend.
10. Website beheerder zorgt dat, indien er informatie over personen op de website wordt geplaatst, de personen hiervoor toestemming hebben verleend.
11. Website beheerder stelt in dat wachtwoorden voor Intranet toegang expireren na één jaar.

Richtlijnen voor de beheerder van Kerk TV

12. **Het liturgisch centrum is altijd in beeld. Dit wordt duidelijk aangegeven. Deze beelden worden ook verzonden via de verschillende diensten. Iedereen die lid is of op bezoek komt weet dat je in het liturgisch centrum in beeld bent. Tenzij iemand hier uitdrukkelijke bezwaren tegen heeft. Dan wordt de camera gericht op het bloemstuk.**
13. **Mededelingen gebed en voorbede wordt van te voren besproken met betrokkenen en is aantoonbaar mee ingestemd. ???? Hier zijn verschillende opvattingen over. Bij controle moet de toestemming aantoonbaar zijn.**

Richtlijnen voor de kerkblad redactie

14. De kerkbladredactie zorgt dat alleen de eigen leden of personen direct gelieerd aan onze gemeente, het kerkblad digitaal ontvangen.
15. Het kerkblad kan naar externe partijen worden gestuurd, maar zonder de secties uit de wijken en uit de gemeente en kerkelijke stand

Richtlijnen voor ambstdragers

16. Gemeenteleden worden alleen dan voorgedragen voor gebed tijdens de erediensten en vermeld in het kerkblad als ze daarvoor schriftelijk toestemming hebben gegeven. Deze toestemming moet bij opvragen aantoonbaar zijn.
17. Toegang tot digitale gegevens van de kerkelijke gemeente zijn beveiligd (bv dmv wachtwoord)
18. Privacy gevoelige informatie mag niet langer bewaard worden dan noodzakelijk. Tevens is deze informatie beveiligd en niet toegankelijk voor gezinsleden en anderen.

Richtlijnen voor het verstrekken van het kerkblad

19. In het handboek worden de ledengegevens beperkt tot naam, adres, dooplid/belijdend lid/catechumeen/geen lid ……

Richtlijnen voor de scriba

20. In de mededelingen worden geen adresgegevens meer gedeeld alleen eventueel de kerkelijke wijk waartoe ze behoren
21. In de instructie voor nieuwe ambtsdragers wordt expliciet aandacht besteed aan de privacyafspraken
22. De scriba zorgt voor publicatie van het privacystatement via het kerkblad en de website
23. Alle huidige gemeenteleden krijgen een brief in hun postvak die hen informeert over de nieuwe regelgeving die tevens uitlegt dat men aan kan geven indien zij hun gegevens niet of beperkt willen hebben opgenomen in de gemeentegids.

Beleidsmaatregelen en besluiten te nemen door de CBZ

24. Vanwege zowel privacy overwegingen, het delen van privacy gevoelige informatie tijdens kerkdiensten, als licentiebeperkingen die openbare uitzending van bepaalde liederen niet toestaat, besluit CBZ om over te gaan tot uitzending van de kerkdiensten altijd achter de login. Om gemeenteleden voor te bereiden op dit besluit zal dit eerst worden gecommuniceerd via het kerkblad en twee keer worden meegedeeld tijdens de diensten met een verwijzing naar de procedure in het kerkblad

## Bijlage 1 Definities en afkortingen

**AP:** Autoriteit Persoonsgegevens.

**Avg:** Algemene verordening gegevensbescherming. Verordening (EU) 2016/679. De Europese opvolger van de Wbp die vanaf mei 2018 van toepassing is.

**Betrokkene:** een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

**Bewerker:** degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

**CBP:** College

**Datalek:** Persoonsgegevens die in handen vallen van derden die geen toegang tot die gegevens (mogen) hebben.

**Derde**: Ieder ander, niet zijnde de betrokkene, de verantwoordelijke of de bewerker, of enig persoon die onder rechtstreeks gezag valt van de verantwoordelijke of de bewerker en gemachtigd is om persoonsgegevens te verwerken.

**FG:** Functionaris voor de Gegevensbescherming.

**Persoonsgegeven:** elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.

**Verantwoordelijke:** de natuurlijke persoon, rechtspersoon of ieder ander die, of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Bij de Zorggroep is de RvB verantwoordelijk, maar dit is gedelegeerd aan de houder van het betreffende informatiesysteem.

**Verwerking** van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling,samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

**Bijlage 2 Registraties administraties**

**Registratie ledenadministratie**

| | |
|---|---|
| **Omschrijving van de verwerking** | Ledenadministratie, gedeeltelijk geautomatiseerde ledenadministratie verwerking via ….. Betreft een administratief dossier |
| **Verantwoordelijke** | Petrakerk Harderwijk |
| **Betrokkene(n)** | Leden van de Petrakerk |
| **Beheerder(s)** | Beheerder ledenadministratie |
| **Bewerker(s)** | |
| **Doelen van de verwerking** | Het voeren van een adequate ledenadministratie voor:<br><br>Het vaststellen van het aantal leden<br><br>Het elkaar kunnen bezoeken van kerkenraadsleden en gemeenteleden<br><br>Het met elkaar kunnen meeleven bij verjaardagen, jubilea, geboorte<br><br>Aanleveren leden gegevens aan vvb bij machtiging zodat de peningmeester het eigen aangegeven bedrag kan innen.<br><br>Geanonimiseerde ledenaantallen doorgeven aan kerkelijk bestand (…….) |
| **Bijzondere persoonsgegevens** | Ja?<br><br>• Doop, met datum en de kerkgemeenschap en naam van de gemeente waarbinnen de doop werd bediend<br>• Belijdenis van het geloof, met datum alsmede de kerkgemeenschap en de naam van gemeente waar belijdenis van het geloof werd gedaan<br>• Kerkelijke inzegening van het huwelijk, met datum en kerkgemeenschap en naam van de gemeente waar de inzegening heeft plaatsgevonden<br>• Indien van toepassing, datum van overkomst uit een andere gemeente of andere kerkgemeenschap<br>• Gegevens ivm het einde van het lidmaatschap van de gemeente<br>• Datum van vertrek dan wel overschrijving naar een andere gemeente met vermelding van de naam van de nieuwe gemeente<br>• Datum van overlijden<br>• Datum van overgang naar een andere kerkgemeenschap<br>• Datum van onttrekking aan de gemeenschap van de kerk<br>• De wijk waartoe betrokkene behoort |
| **Omschrijving persoonsgegevens** | NAW-gegevens<br><br>• Achternaam, roepnamen, doopnamen, voorletters<br>• Geslacht<br>• Geboortedatum en geboorteplaats<br>• Straatnaam, huisnummer, postcode, woonplaats, telefoonnummer en e-mail<br>• Burgerlijke staat |
| | Partner- / familiegegevens |

| | | |
|---|---|---|
| | Bankrekening nummer bij automatische incasso | |
| | BSN ???? | |
| **Gebruiker(s)** | Intern | Extern |
| | Individuele leden<br><br>Penningmeester | |
| **Melding bij College** | ??? | |
| **Bewaartermijn** | ?? | |
| **Doorgifte buiten EU** | Bij vertrek naar buiten EU wel??? | |

Opmerking:

Het uitwisselen van gegevens dient via mail te gaan met wachtwoord. Het vastleggen van gegevens dient in systemen met certificaten te zijn vastgelegd

# Overige Registratie

**Hiervan zou Niels een overzicht maken als ik mij goed kan herinneren**

# Bijlage 3 Protocol datalekken

## Procedure voor het afhandelen van datalekken

Wie een **mogelijk datalek** ontdekt, zal snel onderzoek moeten doen en mogelijk ook meldingen moeten doen aan de overheid en getroffen personen.

Leden van de Petrakerk moeten het datalek **binnen 2 dagen nadat er kennis van is genomen melden** bij de Functionaris Gegevensbescherming (FG) via scriba@petrakerkharderwijk.nl

## Wanneer is sprake van een datalek?

Er is sprake van een datalek als er **bij het beveiligingsincident persoonsgegevens verloren zijn gegaan**, of als onrechtmatige verwerking van de persoonsgegevens redelijkerwijs niet kan worden uitgesloten.

Hiervoor geldt een medlingsplicht bij de Autoriteit Persoonsgegevens.

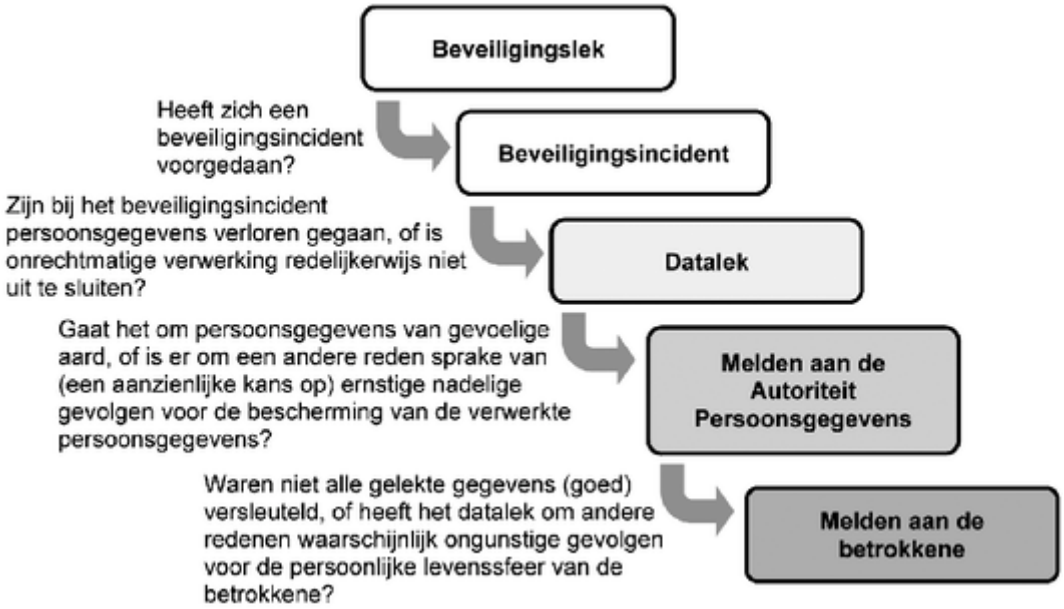
Als alleen sprake is van een **zwakke plek in de beveiliging**, spreken we van een **beveiligingslek** en niet van een datalek.

Daarvoor geldt geen meldingsplicht aan de Autoriteit Persoonsgegevens.

Voorbeelden datalekken:

• moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
• technisch falen (ICT-storingen);
• menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan leden en externen);
• calamiteit (brand datacentrum, wateroverlast);
• verloren USB stick of laptop;
• verzenden van email met emailadressen van alle geadresseerden;
• maar ook het onrechtmatige verwerking van gegevens.

## Triage datalek?



## Handelwijze na melding

De FG registreert iedere melding in het systeem.

De FG neemt daarna contact op met de melder voor aanvullende gegevens over de melding.

Het betreft:

Ø naam van de melder;

Ø datum en tijd van de melding;

Ø aard van de inbreuk (is er aanmerkelijk risico op verlies of onrechtmatige verwerking?);

Ø welke persoonsgegevens vallen onder de melding;

Ø om welk aantal en/of gegevensrecords gaat het;

Ø welke (groepen) personen zijn betrokken bij de melding;

Ø welke maatregelen zijn of worden door de melder getroffen;

Ø welke gevolgen zijn er volgens de melder voor de betrokkenen;

Ø de contactpersoon voor de melding.

· Door FG wordt een eerste analyse gedaan.

· Als het om persoonsgegevens gaat (datalek), dan wordt het incident bij de kerkenraad gemeld.

· Het incident als datalek geadministreerd.

· De volgende gegevens worden besproken en vastgelegd:

o de gegevens die door de FG zijn vastgelegd bij het aannemen van de melding

o de noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer;

o hetgeen gemeld gaat worden bij het CBP door de FG (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records):

- de mogelijke gevolgen voor de betrokkenen;
- de maatregelen die de Petrakerk neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
- de maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
- contactgegevens voor betrokkenen;

o de wijze van afhandeling intern, inclusief communicatie naar melder, kerkenraad

o of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;

o het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit de Petrakerk zelf, een bewerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst wordt extern juridisch advies ingewonnen;

o hetgeen intern gecommuniceerd wordt, op welk moment;

o hetgeen extern gecommuniceerd wordt, op welk moment. Er wordt vastgesteld of de pers geïnformeerd moet worden;

o of naast het CBP ook andere partijen geïnformeerd worden;

o op welke wijze er intern wordt gerapporteerd, inclusief actiehouder;

o of eventuele schade is gedekt door de verzekeringspolis.

· De FG verzorgt de afhandeling van het security incident, waarbij bewijsmateriaal of informatie voor het afhandelen van het datalek in een veilige omgeving wordt bewaard.

· De FG zorgt voor afhandeling van het privacy incident.

· De FG maakt samen met de Kerkenraad een afweging of het incident gemeld moet worden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene.

## Melden

Meldingen bij de AP worden gedaan door de FG.
Het zo nodig informeren van de betrokken personen wordt ook gedaan door de FG.

## Melden aan de Autoriteit Persoonsgegevens

Niet ieder datalek hoeft te worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet een melding gedaan worden aan de Autoriteit Persoonsgegevens **als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens**.

*(Bij de interpretatie van onderstaande begrippen volgen wij de "Beleidsregels voor toepassing van artikel 34a van de Wbp", van de Autoriteit Persoonsgevens)*

*De Wet Bescherming Persoonsgegevens gebruikt een brede definitie van persoonsgegevens.* ***Elk gegeven dat herleidbaar is tot een natuurlijk persoon, is een persoonsgegeven****. Dit betreft namen, adressen, kentekens, telefoonnummers, IP-nummers, email-adressen, biometrische kenmerken, een combinaties van specifieke voorkeuren.*

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er **persoonsgegevens van gevoelige aard** zijn gelekt, dan is over het algemeen een melding noodzakelijk.

Persoonsgegevens van gevoelige aard zijn **bijvoorbeeld**:

· Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp
Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

- Gegevens over de financiële of economische situatie van de betrokkene
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden

- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.

- Gebruikersnamen, wachtwoorden en andere inloggegevens
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- Gegevens die kunnen worden misbruikt voor (identiteits)fraude
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Ook andere factoren, zoals de **hoeveelheid gelekte persoonsgegevens** per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden.

Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het zelfs mogelijk dat een datalek moet worden gemeld waarbij de persoonsgegevens van slechts één persoon betrokken zijn.

De **melding** moet worden gedaan zonder onnodige vertraging en zo mogelijk **niet later dan 72 uur na de ontdekking van het datalek**.

Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. Via dit webformulier kan de melding later nog worden aangevuld of ingetrokken.

**Melden aan betrokkenen**

Als een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat dit datalek ook moet worden gemeld aan de betrokkene. De wet geeft hiervoor als richtlijn dat het datalek moet worden gemeld aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

De wet schrijft voor dat de melding aan de betrokkene onverwijld moet worden gedaan, zodat de betrokkene naar aanleiding van de melding maatregelen kan nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover geïnformeerd is, hoe eerder deze in actie kan komen.

Als er passende technische beschermingsmaatregelen zijn genomen (zoals encryptie en hashing), waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege blijven.

**Vervolgstappen**

Zodra de melding aan de Autoriteit Persoonsgegevens en aan de betrokkenen is gedaan, is voldaan aan de meldplicht en zal de FG het privacy incident afsluiten.

**Rapportage**

De FG houdt een register bij van alle gemelde datalekken en de actuele status daarvan.

Rapportage over datalekken wordt meegenomen in een jaarrapportage, die door de FG wordt opgesteld.