



INRICHTING PRIVACY

Inhoud:

1.	ALGEMEEN.....	2
2.	ORGANISATIE PRIVACY.....	2
2.1	Positie en taken functionaris gegevensbescherming in gemeente	2
2.2	Toetsingskader	2
2.3	Register voor datalekken	2
2.4	Beheren toestemmingen	3
3.	PROCESSEN VOOR PRIVACY	4
3.1	Behandelen verzoek om inzage of klacht	4
3.2	Behandelen Datalek	4
3.3	Beheerprocessen	4
4.	PRIVACYMAATREGELEN IN DE GEMEENTE.....	5
4.1	Verantwoordelijkheden voor persoonsgegevens	5
4.2	Maatregelen voor privacybescherming	6
5.	RISICOANALYSE EN MAATREGELEN.....	6

Revisiehistorie			
Versie	Datum	status	Aangebrachte wijzigingen
0.1	08-10-2018	concept	eerste concept
0.2	00-11-2018	concept	resultaten bespreking projectgroep Privacy 11-10 verwerkt
0.3	06-11-2018	concept	opmerkingen Pieter Ijlst verwerkt
0.4	10-12-2016	concept	opmerkingen Ada verwerkt en informatie van Autoriteit Persoonsgegevens over toestemmingen
1.0	08-02-2019	definitief	Goedgekeurd door kerkenraad

1. Algemeen

Over privacy zijn drie documenten opgesteld voor verschillende doelgroepen. Ze worden op het openbare deel van de website van De Lichtzijde geplaatst.

1. De privacyverklaring beschrijft welke persoonsgegevens worden gebruikt in De Lichtzijde en met welk doel. Het geeft gemeentelieden inzicht in welke gegevens over hen zijn geregistreerd.
2. Inrichting privacy beschrijft de organisatie en processen rond privacy in De Lichtzijde. Dit is vooral een document voor de interne besturing. Het beschrijft o.a. hoe verzoeken en datalekken worden behandeld en hoe het toezicht op de privacy is geregeld.
3. De Do's en Dont's beschrijven hoe gebruikers met persoonsgegevens moeten omgaan. Dit is van belang voor alle gebruikers van persoonsgegevens van gemeentelieden.

In dit document, Inrichten Privacy, worden de organisatie rond privacy beschreven met de taken van de privacyfunctionaris, de relatie naar de kerkenraad, het toetsingskader en het register voor datalekken. Aansluitend worden de processen beschreven voor de privacyfunctionaris, bijvoorbeeld voor het behandelen van een verzoek en een melding van een datalek.

Daarna wordt ingegaan op de processen, die persoonsgegevens gebruiken en de privacy risico's en maatregelen om deze beheersbaar te maken.

2. Organisatie Privacy

2.1 Positie en taken functionaris gegevensbescherming in gemeente

De kerkenraad is verantwoordelijk voor privacy in de gemeente en de contacten naar de Autoriteit Persoonsgegevens. Om de privacy van de gemeentelieden te waarborgen zorgt de kerkenraad ervoor dat er voldoende maatregelen worden getroffen bij alle processen, die door of namens hem worden uitgevoerd. Dit betreft o.a. de werkzaamheden van hemzelf, de ouderlingen, de diakenen, de vertrouwenspersonen, de jeugdwerker en jeugdleiding, commissies. Elke raad, commissie, of gemeentelid die binnen de gemeente actief is, zorgt zelf voor het maken van afspraken over privacy en ziet er op toe dat deze worden nageleefd. De kerkenraad besluit over de afspraken.

De kerkenraad stelt een functionaris gegevensbescherming aan. Deze heeft een adviserende rol naar de kerkenraad en rapporteert aan de voorzitter van de kerkenraad.

De taken van deze functionaris zijn:

- Informeren en adviseren van de kerkenraad en de gemeentelieden over de AVG;
- Toezien op de naleving van de AVG;
- Behandelen van verzoeken van gemeentelieden over privacy;
- Registreren en rapporteren privacy-incidenten en het bijhouden van het register datalekken;
- Opstellen en onderhouden van de documenten over privacy.

Uitgangspunten zijn verder:

- Correspondentie voor en van de functionaris gaat via de scriba.
- De functionaris stelt zich onafhankelijk op.
- De functionaris verkrijgt alle medewerking van betrokken organen, ambtsdragers en gemeentelieden bij het uitoefenen van de taken.

2.2 Toetsingskader

De functionaris hanteert het volgende toetsingskader bij het uitoefenen van de taken:

- De privacyverklaring van De Lichtzijde;
- De Do's en Dont's van de Lichtzijde;
- Bij bewerking van gegevens door derden moet het bedrijf ISO 27001 gecertificeerd zijn. Dit certificaat garandeert een onafhankelijke controle op de naleving van de nieuwe privacywetgeving (bewerkerovereenkomst AVG).
- De wet- en regelgeving over de AVG en nadere toelichting daarop van de Autoriteit Persoonsgegevens. Deze prevaleert boven de hiervoor genoemde documenten.

2.3 Register voor datalekken

In het register voor datalekken worden de volgende gegevens geregistreerd:

- Datum van de constatering;
- Volgnummer;

- Korte beschrijving van het datalek en de oorzaak van het ontstaan;
- Vermeld naam en contactgegevens van de persoon die de melding heeft gedaan;
- Vermelden welke andere organisaties en/of personen betrokken zijn bij het incident;
- Korte omschrijving van de mogelijke gevolgen van het datalek (bijvoorbeeld: gegevens gehackt, gegevens verloren, gevoelige informatie bekend bij derden);
- Beschrijving van de genomen maatregelen om het datalek aan te pakken en herhaling te voorkomen;
- Datum gemeld bij Autoriteit Persoonsgegevens (binnen 72 uur);
- Aangeven of en op welke manier het datalek is gemeld aan de betrokkene(n);
- Het verdient aanbeveling om naast het register voor elk datalek een dossier aan te leggen, waarin alle relevante correspondentie met betrokkenen wordt opgeslagen.

2.4 Beheren toestemmingen

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht geworden. Kern is dat de bescherming van persoonlijke levenssfeer meer dan nu gewaarborgd moet worden door organisaties, ook door kerken. De landelijke organisaties van de kerken zijn al maanden met de voorbereiding bezig. Ze zijn ook nog in gesprek over de interpretatie van de AVG voor kerken met de Autoriteit Persoonsgegevens (AP), die toezicht houdt namens de overheid. En dat blijkt niet eenvoudig te zijn, want over onderwerpen als welke gegevens delen en is al dan niet toestemming nodig en de wijze waarop, is nog steeds geen volledige duidelijkheid. De leden van een kerk vormen namelijk een gemeenschap en willen juist op elkaar betrokken zijn. Ze delen daarom met elkaar allerlei persoonlijke gegevens over gezondheid, werk, onderwijs, welzijn, ouders, kinderen, enz. Zo krijgt de liefde voor elkaar en meeleven met elkaar praktische invulling. Dat is een heel andere context dan een relatie tussen een klant en leverancier of tussen een gebruiker en een internetdienstverlener als Facebook of Google. Met de AP is contact geweest over de wijze waarop toestemming verkregen zou kunnen worden. In de PrivacyVerklaring is beschreven waarvoor toestemming nodig is en de wijze waarop. Hierna wordt een overzicht gegevens inclusief de verantwoordelijke voor het beheer van de toestemming.

Situatie	Soort toestemming	Verantwoordelijke voor verkrijgen en beheren toestemming
Nieuwsbrief	mondeling of schriftelijk toestemming	lid kerkenraad, lid kerkenraad
Gemeentegids op besloten website	de gemeente heeft toestemming verkregen van de gemeentevergadering.	kerkenraad, scriba
Gemeentegids op papier	Voor leden voor wie het niet mogelijk is de website in te zien, wordt in principe jaarlijks een afdruk gemaakt, die in een gesloten envelop aan hen wordt aangeboden. Dit valt onder het briefgeheim.	kerkenraad, scriba
Geluidopnames van diensten	gewone kerkdiensten zijn openbaar. Voorbeden en dankzegging voor personen gebeurt op mondeling of schriftelijk verzoek.	lid kerkenraad, lid kerkenraad
Beeldopnames van kerkdiensten	Beeldmateriaal kan op de besloten website worden geplaatst met de vermelding dat dit uitsluitend voor gebruik binnen de gemeente is. Voorafgaand aan het openbaar maken kunnen de volgende maatregelen worden getroffen: 1. Breng alleen de rug van bezoekers in beeld.	kerkenraad, scriba

	2. Wijs een deel van de kerkzaal aan waar bezoekers ook met gezicht in beeld kunnen komen en zorg dat zij hierover goed geïnformeerd zijn.	
Op website staan foto's van bezoekers van de kerk.	schriftelijk toestemming	kerkenraad, scriba

3. Processen voor privacy

3.1 Behandelen verzoek om inzage of klacht

Met dit proces worden de volgende verzoeken voortvloeiende uit onderstaande rechten behandeld (zie Privacy Verklaring):

1. Het recht op dataportabiliteit.
2. Het recht op vergetelheid.
3. Recht op inzage.
4. Recht op rectificatie en aanvulling.
5. Het recht op beperking van de verwerking:
6. Het recht met betrekking tot geautomatiseerde besluitvorming en profilering.
7. Het recht om bezwaar te maken tegen de gegevensverwerking.

De volgende processtappen worden doorlopen:

- a. De scriba ontvangt het schriftelijke verzoek en geeft dit door aan de functionaris gegevensbescherming (FG);
- b. De FG overlegt met betrokkene over het verzoek;
- c. De FG overlegt met de registratiehouder over het verzoek en zorgt voor contact tussen betrokkene en registratiehouder;
- d. Het verzoek wordt gehonoreerd of met toelichting afgewezen;
- e. Betrokkene wordt schriftelijk geïnformeerd over de afhandeling van het verzoek, concept stelt FG op en wordt door kerkenraad verzonden.

3.2 Behandelen Datalek

Als een datalek wordt gemeld worden de volgende processtappen doorlopen:

- a. De scriba ontvangt de schriftelijke melding en geeft dit door aan de functionaris gegevensbescherming (FG);
- b. De FG overlegt met betrokkene over de melding en werkt het register datalekken bij;
- c. De FG overlegt met de registratiehouder(s) over de melding en zorgt voor contact tussen betrokkene en registratiehouder(s);
- d. De melding wordt binnen 72 uur doorgegeven aan de Autoriteit Persoonsgegevens (AP);
- e. Naar aanleiding van de melding wordt overlegd met de mogelijke veroorzakers en of aanvullende maatregelen op het gebied van privacy getroffen moeten worden;
- f. De FG beantwoordt vragen van de AP in overleg met de kerkenraad;
- g. Betrokkene wordt schriftelijk geïnformeerd over de afhandeling van de klacht, concept stelt FG op en wordt door kerkenraad verzonden.

Mogelijk wordt juridisch bijstand gezocht. In geval de AP een boete oplegt, wordt overwogen een bezwaar in te dienen.

3.3 Beheerprocessen

De volgende beheerprocessen worden onderkend:

- Rapporteren aan de kerkenraad over privacy.
- Toetsen of de afspraken op gebied van privacy en schonen van stukken met persoonsgegevens worden nageleefd;
- Volgen van de ontwikkelingen op het gebied van privacy en zonodig wijzigingen doorvoeren in de privacydocumenten.
- Communiceren over privacy in de gemeente.

- Actualiseren van de risicoanalyse.

4. Privacymaatregelen in de gemeente

4.1 Verantwoordelijkheden voor persoonsgegevens

Persoonsgegevens zijn alle gegevens die betrekking hebben op een persoon. De AVG is echter alleen van toepassing, als sprake is van verwerking van persoonsgegevens. Dat is het geval wanneer persoonsgegevens zijn opgenomen in een bestand of het de bedoeling is dat dat zal gebeuren en/of wanneer de gegevens geautomatiseerd worden verwerkt. Zuiver persoonlijke aantekeningen vallen niet onder het inzagerecht evenmin als wat losse papieren op het bureau met daarin wat namen of een puur mondelinge overdracht van gegevens. Zodra er structuur wordt aangebracht in de gegevens is de AVG echter van toepassing.

Bijvoorbeeld voor vertrouwenspersonen betekent dit dat aantekeningen van gesprekken met cliënten niet onder de AVG vallen als het puur persoonlijke aantekeningen zijn waar verder niets mee gebeurt. Zodra de aantekeningen echter worden bijgehouden, bijvoorbeeld ten behoeve van een geanonimiseerd jaarverslag of simpelweg om overzicht te houden, is de AVG van toepassing. Het maakt daarbij niet uit of de aantekeningen alleen op papier worden bewaard of ook in de computer.

In de privacyverklaring wordt benoemd welke persoonsgegevens worden gebruikt in De Lichtzijde en met welk doel. Het geeft gemeentelieden inzicht in welke gegevens over hen zijn geregistreerd. De verantwoordelijke hiervoor staat in onderstaande tabel.

Persoonsgegevens	Verantwoordelijke	Uitvoering door
Algemene Organisatie		
Ambtsdragers en verkiesbare ambtsdragers	Kerkenraad	Scriba
Ledenadministratie	Kerkenraad	Scriba
Verwerkingen vanwege het plaatselijk leven en werken van de kerk		
Nieuwsbrieven	Kerkenraad	Redactie nieuwsbrief
Zieke personen in nieuwsbrief	Kerkenraad	Lid kerkenraad
Gemeentegids	Kerkenraad	Scriba
Tijdens kerkdienst worden namen van leden van de gemeente genoemd	Kerkenraad	Lid kerkenraad
Gepubliceerde opnames van kerkdiensten	Kerkenraad	Lid Commissie van Beheer
Op website staan functionarissen van de kerk met foto en gegevens	Kerkenraad	Scriba (toestemming), Webmaster (plaatsing)
Op onze website staan foto's van bezoekers van de kerk	Kerkenraad	Scriba (toestemming), Webmaster (plaatsing)
Gemeentelieden ontvangen informatie voor een financiële bijdrage of toezegging	Kerkenraad, Diaconale Raad	Penningmeester Commissie van Beheer, Penningmeester DR
Hulpaanvragen bij de diaconie worden opgenomen in een administratie	Diaconale Raad	Penningmeester DR
De gemeente of de diaconie gebruikt camera's om te filmen wat er gebeurt.	Kerkenraad	Commissie van beheer
Aantekeningen van ouderling over pastorale gesprekken met gemeentelieden	Kerkenraad	Ouderling, Predikant
Aantekeningen van diaken over diaconale gesprekken met gemeentelieden	Diaconale Raad	Diaken
Verslagen van kerkenraad, diaconale raad en wijkteamoverleg	Kerkenraad, Diaconale Raad	Scriba, Secretaris DR, Wijkteam
Aantekeningen van jeugdwerker over gesprekken met jongeren	Kerkenraad	Jeugdwerker

Voorsnog wordt er vanuit gegaan dat vertrouwenspersonen alleen persoonlijke aantekeningen maken en geen persoonsregistratie voeren.

4.2 Maatregelen voor privacybescherming

Op welke wijze de privacy wordt gewaarborgd moet ook worden afgesproken. De in § 4.1 genoemde verantwoordelijke legt deze afspraken vast en ziet er op toe dat ze worden nageleefd. De afspraken betreffen de volgende onderwerpen (auditformulier):

- Welke persoonsgegevens?
- Wie beschikt over de gegevens, wie heeft toegang?
- Welke veiligheidsprocedures zijn er?
- Hoe lang worden persoonsgegevens bewaard?
- Wat gebeurt er als een gegevensgebruiker aftreedt?
- Wat gebeurt er bij verhuizing, overlijden, onttrekking, e.d.

De afspraken worden zo vastgelegd, dat ze raadpleegbaar zijn voor verantwoordelijken en uitvoerenden en overdraagbaar zijn aan nieuwe uitvoerenden. De functionaris gegevensbeheer gebruikt ze ook bij toetsing.

5. Risicoanalyse en maatregelen

Met persoonsgegevens moet zorgvuldig worden omgegaan. Ondanks goed afspraken zijn er toch risico's te onderkennen. Deze worden hierna benoemd en de maatregelen om de risico's beheersbaar te maken. Onderscheiden worden risico's in:

- Verwerking van gegevens;
- Gebruik van ontvangen gegevens;
- Technische hulpmiddelen.

Risico	Maatregelen
Verwerking van gegevens	
Afspraken zijn niet bekend	<ul style="list-style-type: none"> ○ Afspraken vastleggen, communiceren en via website toegankelijk maken ○ Toetsen of afspraken worden nageleefd
Fout in verzending van gegevens	<ul style="list-style-type: none"> ○ Werken met contactgroepen voor verzending
Gegeven toestemming wordt ontkend	<ul style="list-style-type: none"> ○ Duidelijke afspraken over vastleggen toestemming ○ Goed heheer van de gegeven toestemmingen
Gebruik van ontvangen gegevens	
Digitaal verstrekken gegevens aan personen die niet tot doelgroep behoren, zowel binnen de gemeente als naar buiten toe	<ul style="list-style-type: none"> ○ Afspraken maken over doelgroep ○ Afspraken communiceren ○ Gebruik BCC bij verzending ○ Vernietigen gegevens bij verlaten van doelgroep
Op papier verstrekken gegevens aan personen die niet tot doelgroep behoren	<ul style="list-style-type: none"> ○ Vernietigen van op papier verstrekte gegevens ○ Zo min mogelijk gegevens op papier verstrekken
Technische hulpmiddelen	
Diefstal, hacken, verkoop of dumpen van PC, tablet of smartphone	<ul style="list-style-type: none"> ○ Beveiligen met wachtwoord ○ Verwijderen persoonsgegevens als niet meer nodig is
Door gebruik Dropbox of Google Drive kunnen autoriteit in de VS toegang tot gegeven eisen	<ul style="list-style-type: none"> ○ Geen persoonsgegevens in Dropbox of Google Drive, tenzij versleuteld
Ledenregistratie breder toegankelijk o.a. voor wijkouderling	<ul style="list-style-type: none"> ○ Stoppen met verspreiden van Ekklesia
Misbruik interne website	<ul style="list-style-type: none"> ○ Accountbeheer met toegang voor alleen leden en leden Kompas ○ Expliciet vermelden dat alleen voor intern gebruik is

Risico	Maatregelen
	<ul style="list-style-type: none"><li data-bbox="810 226 1278 275">○ Periodiek verwijderen van lang niet gebruikte logins