Algemene Verordening Gegevensbescherming (AVG)

General Data Protection Regulation (GDPR)

Inhoud ..... **Fout! Bladwijzer niet gedefinieerd.**

Inleiding

Op 25 mei gaat de Europese General Data Protection Regulation (GDPR) en de Nederlandse Algemene Verordening Gegevensbescherming (AV) in werking. Deze verordening heeft consequenties voor alle organisaties, ook kerken. Vanaf 25 mei 2018 moet elke organisatie, stichting of kerk voldoen aan deze wet! Deze wet vraagt om uw serieuze aandacht en tijdige aanpassingen om aan de eisen te voldoen. Bij niet voldoen kunnen er hoge boetes zijn. In deze notitie vindt u een uitleg over wat het inhoudt, wat u moet doen met tips, verwijzingen en voorbeelden.

Het is veel informatie, in het kort komt het er op neer dat u moet:

- Bepalen welke persoonsgegevens uw kerk/organisatie gebruikt
- Controleren of de manier waarop persoonsgegevens gebruikt wordt voldoet aan de AVG en dit zo nodig aanpassen
- Een privacy-statement opstellen
- Leden en bezoekers op de hoogte stellen van het beleid en waar nodig toestemming vragen voor gebruik van persoonsgegevens.

Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect te herleiden zijn tot één of meer personen waardoor personen identificeerbaar zijn. Naam, adres, postcode, woonplaats, telefoonnummer geslacht, geboortedatum etc. Voor gevoelige persoonsgegevens zijn extra regels: ras, geslacht, geloofsovertuiging, pastorale informatie etc. Het gaat niet alleen om persoonsgegevens in tekst maar ook in beeld en geluid. Gegevens kunnen op papier staan, in kasten opgeborgen, op computers laptops, online, USB-sticks, mobiele telefoons (what's app!) etc.

Kerken mogen relevante gegevens gebruiken en bewaren. Een ledenlijst of gemeentegids kan relevant zijn. De kerk/organisatie mag persoonsgegevens doorgeven aan anderen die tot de kerk behoren. Voorbeeld: een lijst met namen en telefoonnummers van deelnemers aan een bijbelcursus. De kerk/organisatie mag persoonsgegevens aan mensen of organisaties buiten de kerk alleen verstrekken als er het mag van de wet. Of als iemand daarvoor toestemming heeft gegeven.

Personen mogen altijd hun eigen gegevens inzien maar niet de gegevens van een ander. Vanwege de aard van de kerk/ organisatie mogen bestuur, medewerkers en/of vrijwilligers relevante gegevens inzien. Een persoon mag niet zomaar gegevens delen die hem/haar in vertrouwen zijn gegeven. Er moet een goede reden voor zijn. Wanneer er dossiers zijn moet geregeld zijn wie toestemming voor inzage heeft binnen de kerk/organisatie. Dit moet beschreven worden in het privacy beleid.

https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/recht-op-inzage

Privacy-statement

Iedere kerk moet nadenken over :

- Welke gegevens wil ik hebben?
- Voor welk doel gebruik ik het?
- Waar, hoe en hoelang sla ik de gegevens op?
- Is dat veilig?
- Kan iemand makkelijk zijn/haar persoonsgegevens opvragen, wijzigen en verwijderen?
- Is iedereen op de hoogte?
- Kan ik zien wanneer ik welke gegevens gewijzigd heb?

Met deze informatie maakt de kerk/organisatie een privacy statement. Een handige tool hiervoor is:

https://www.isimedia.nl/zo-maak-je-je-privacyverklaring-avg-proof-zet-hem-op-je-website/

In de bijlage vindt u een voorbeeld van SKIN-Rotterdam dat met deze tool is gemaakt.

Functionaris

Het aanstellen van een officiële functionaris is niet verplicht voor kerken en organisaties waarbij gegevensverwerking niet de “corebusiness” is. Het is wel handig om iemand te benoemen die de zaken rond privacy coördineert en controleert. Deze functionaris kan met behulp van het stappenplan en de checklist AVG (bijlagen) direct aan de slag.

Datalekken

Iedere vorm van verlies, misbruik of diefstal van persoonsgegevens kan een datalek zijn.
Voorbeelden:

- Een e-mail verzonden naar verkeerde adressen
- Een zakelijke smartphone met foto’s en adressen die je hebt verloren (de privetelefoon, bedoeld voor uitsluitend persoonlijke doeleinden weer niet)
- Een oude computer die je met niet gewiste harde schijf wegdoet
- Illegaal verkregen adresbestanden
- Een USB-stick die je hebt verloren
- Een inbraak op je website waar persoonsgegevens te vinden zijn
- Geslaagde cyberaanvallen
- Een gestolen uitgeprinte lijst met adressen
- Uitgelekte computerbestanden
- Het stelen van een laptop uit een afgesloten kluisje

Datalekken bij **persoonsgegevens van gevoelige aard** moeten binnen 72 uur gemeld worden bij de autoriteit persoonsgegevens. Datalekken moeten meestal ook gemeld worden aan betrokkenen. Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

De praktijk

Foto en video

Herkenbaarheid van publiek op foto's of video staan is meestal niet relevant voor de kerk/organisatie maar laat wel iets zien van de activiteit en de sfeer. Beeldmateriaal van de rug van mensen of wanneer mensen in een grote groep "wegvallen" valt onder niet herkenbaar.

Voor het gebruik van foto's en video's waar mensen wel herkenbaar op staan moet toestemming gevraagd worden. Bij leden kan dat eenmalig gevraagd worden met een schriftelijke bevestiging of accepteren van de privacy-statement (papier, email, knop op website). De toestemming moet ingetrokken kunnen worden. Dat betekent dat geregistreerd moet worden wie toestemming heeft gegeven en wie niet. Bij open bijeenkomsten kan persoonlijk toestemming worden gevraagd, bijvoorbeeld door een formulier of door een statement op de presentielijst op te nemen. Zie ook bij uitzenden kerkdiensten. Dit geldt ook voor foto's en video's die al gepubliceerd zijn.

Uitzending kerkdienst (audio en beeld, live, YouTube, etc.)

De AVG staat streaming van diensten of andere activiteiten toe wanneer dit relevant is voor de organisatie. Neem daarom op in het privacy-statement waarom de kerk/organisatie dit belangrijk vindt en hoe zij hier mee omgaat. Iedereen die herkenbaar in beeld komt moet wel toestemming hebben gegeven (zie ook hierboven). Naast privacy moet ook rekening gehouden worden met auteursrechten op preken en muziek. Wanneer het niet nodig is dat de uitzending openbaar is zet deze dan achter een toegangscode. Aandachtspunten en tips:

- Geef aan met bordjes dat er geluids- of beeldopnamen gemaakt worden/kan worden (camerabordjes).
- Zend geen informatie uit met persoonsgegevens (zieken, overledenen etc.), Zet eventueel de microfoon dan uit.
- Let erop wanneer camera's aan en uit staan (denk ook aan cameratoezicht omwille van de veiligheid)
- Denk na over de cameraposities. Een ronddraaiende camera die mensen individueel herkenbaar in beeld brengt, vraagt een andere benadering dan vaste camera's die het kerkgebouw of alleen de voorganger in beeld brengt. Markeer eventueel de ruimte die je in beeld brengt (bijvoorbeeld alleen de eerste rij).
- Denk na over hoelang uitzendingen online beschikbaar zijn.
- Denk na over opslag en bewaartermijnen offline.

- Als er privacybezwaren zijn, bewaar de uitzending dan niet (maar verwijder de stream na bijv. 1 uur)
- Is er een bewerkersovereenkomst met de streaming leverancier?
- Betrek andere rechten (denk aan auteurs- en naburige rechten, bijv. over het uitzenden van muziek)
- Check het huidige beeld en audiomateriaal dat online staat, verwijder het zo nodig of vraag alsnog toestemming aan personen om in beeld te zijn.

Magazine / kerkblad / Nieuwsbrief

In een magazine/nieuwsbrief voor leden mogen relevante persoonsgegevens van leden staan. Wanneer er twijfel is over de relevantie maar wilt u het toch graag publiceren, vraag dan toestemming en respecteer wanneer nee gezegd wordt. Let op dat er niet-leden ook een abonnement kunnen hebben op een interne nieuwsbrief bijvoorbeeld journalisten.

Een nieuwsbrief mag toegestuurd worden naar leden zonder dat zij zich hebben opgegeven maar zij moeten zich wel kunnen afmelden. Dat betekent dat er een registratie bijgehouden moet worden.

De kerk/organisatie mag niet ongevraagd een nieuwsbrief sturen naar niet-leden, zij moeten zichzelf abonneren en ook zichzelf kunnen afmelden. Als iemand zich voor de ene lijst heeft opgegeven, dan is het niet zomaar toegestaan voor een andere mailing nieuwsbrieven te versturen.

Er mogen alleen relevante gegevens voor het versturen nieuwsbrief van de nieuwsbrief gevraagd worden en de gegevens mogen niet voor een ander doel gebruikt worden. Adressen die je van derden hebt gekregen mag je niet zonder toestemming van de personen zelf gebruiken.

Tips

Algemeen

- Zorg ervoor dat iemand bewust een actie moet uitvoeren om akkoord te gaan met het opslaan en verwerken van gegevens. Bijvoorbeeld een ja-vinkje op akkoord privacystatement.
- Zorg ervoor dat iemand eenvoudig zijn/haar voorkeuren kan wijzigen.
- Zorg ervoor dat je inzage kunt geven in de gegevens die je van iemand hebt geregistreerd

Nieuwsbrief

- Zorg ervoor dat aan- en afmelden voor een nieuwsbrief of mailing makkelijk gaat

Website

- Laat geen persoonsgegevens zien van mensen die geen functie in de kerk hebben
- Gebruik zoveel mogelijk kerkmailadressen ipv persoonlijke mailadressen bv pastor@kerk.nl - Vraag schriftelijke toestemming voor beeldmateriaal waar mensen herkenbaar in beeld zijn Zie boven.
- Publiceer magazine/nieuwsbrief zonder persoonsgegevens online.

Email

- Mail naar groepen met de mailadressen in de Bcc (Blind cc)
- Stel in dat een reply op email wordt verzonden zonder dat alle eerdere mails “er onder” zijn (of verwijder handmatig oude mailtjes die “eronder” zijn)

Facebook

- Facebook instellingen AVG-proof maken: https://www.isimedia.nl/facebook-en-de-avgcheck-je-instellingen/
- Facebook gegevens downloaden om te bekijken wat je wilt verwijderen. https://www.isimedia.nl/wat-weet-facebook-van-jou-zo-download-je-al-je-facebookgegevens/
- Facebook verwijderen: https://www.isimedia.nl/klaar-met-facebook-verwijder-je-accountof-check-je-privacy-deletefacebook/
- Alle berichten facebook persoonlijke account verwijderen: https://www.isimedia.nl/hoe-kunje-meerdere-berichten-van-facebook-in-een-keer-verwijderen/
- Alle berichten van je facebookpagina verwijderen: https://www.isimedia.nl/zo-verwijderberichten-facebook-pagina/

Google Analytics

- Kiezen bewaartermijn data google analytics https://www.isimedia.nl/google-analytics-en-deavg-dit-verandert-er/
- Handleiding privacy-vriendelijk instellen google analytics: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_privacyvriendelijk_instellen_google_analytics_mrt_2018.pdf

Cookies

- Cookies instellingen op website AVG-proof maken: https://www.isimedia.nl/nieuwecookiewet-wat-moet-je-aan-je-website-veranderen/

Softwarepakketen van derden

- Controleer of het bedrijf ISO 27001 gecertificeerd is
- Regel afspraken rond persoonsgegevens in de overeenkomst.

Bronnen en verdere informatie

Nederlands:

- https://www.protestantsekerk.nl/actief-in-de-kerk/besturen/kerkenraad/privacy

- https://diaconaalsteunpunt.nl/kerk-en-avg/
- https://www.steunpuntkerkenwerk.nl/avg/
- https://www.isimedia.nl/privacy-en-de-kerk-veelgestelde-vragen-over-de-nieuweprivacywetgeving-avg/
- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europeseprivacywetgeving
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf

English:

- http://www.parishresources.org.uk/gdpr/

Bijlagen:

Nederlands:

- Stappenplan AVG-proof
- Checklist AVG
- SKIN-Rotterdam privacy statement VOORBEELD

English:

- Data protection requirements
- GDPRchecklist
- Sample-Privacy-Notice

Stappenplan AVG proof

Stap 1: maak beleid en spreek erover

Privacy is van belang. Juist ook in de kerk waar mensen soms op hun kwetsbaarst zijn. Een goed privacybeleid zorgt ervoor dat de persoonsgegevens van iedereen gewaarborgd zijn, dat gegevens beveiligd worden en alleen worden gebruikt als dat in de kerk nodig is. De AVG laat alle ruimte voor kerken en organisaties om haar taak te vervullen en gebruik te maken van persoonsgegevens, zolang de waarborgen maar op zijn plaats zijn.

Stap 2: het informeren van mensen en het privacy-statement

Iedereen die met de kerk te maken heeft moet weten wat er met zijn of haar gegevens gebeurt. Als u gebruik maakt van formulieren (zowel online als op papier) waar mensen hun gegevens achterlaten moeten mensen geïnformeerd worden over hoe er met hun privacy om wordt gegaan.

Stap 3: het bewaren van gegevens: maak beveiliging standaard en weet wat er gebeurt

Beveiliging moet standaard zijn. U moet weten wie welke gegevens heeft en waarom deze persoon de gegevens gebruikt. U moet er ook voor zorgen dat de informatie niet zomaar voor iedereen toegankelijk is: zorg voor een af te sluiten kast, zorg voor een afgesloten gedeelte op de website en maak geen gebruik van inlogcodes die meerdere mensen hebben. Gratis diensten als google drive of dropbox kunnen gebruikt worden, zolang maar helder is wie er toegang hebben tot de gegevens en de gegevens niet zomaar op straat komen te liggen.

Beveiliging betekent ook het verwijderen van oude bestanden. Als u bijvoorbeeld gegevens uit het ledenregistratiesysteem haalt en op uw computer downloadt, moet u die na gebruik weer verwijderen. Maar het gaat ook om het verwijderen van oud-leden die zijn verhuisd, vertrokken of overleden. Meer informatie over wanneer u gegevens dient te verwijderen kunt u bij de Autoriteit Persoonsgegevens vinden.

Stap 4: het delen van gegevens: alleen als het nodig is

Als het niet in de statuten staat neem dan in het privacy-statement op dat iedereen die met gegevens werkt is gehouden tot geheimhouding. Dan hoeft niemand daarvoor een formulier te ondertekenen, die regel is op iedereen van toepassing. Gegevens die u binnen de kerk deelt mogen niet (zomaar) doorgegeven worden. Alleen als het valt binnen de taak van de kerk en het nodig is, mag u de gegevens delen. De regels wanneer het delen van gegevens valt binnen de taak van de kerk staan in uw privacy-statement.

Als u de gegevens ergens anders voor wilt gebruiken dan binnen de taak van de kerk valt en in uw privacy-statement is te lezen, dan moet u expliciet toestemming vragen aan degene wiens gegevens u wilt gebruiken.

Stap 5: meld het als het fout gaat/meld datalekken

Soms gaat het mis. Misschien heeft u per ongeluk een deel van de ledenlijst naar een verkeerd emailadres gestuurd. Of zijn de namen van zieke gemeenteleden toch op de website terecht gekomen.
In zo'n geval moet u nagaan of u een melding moet maken. Meer informatie:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Bron: https://www.protestantsekerk.nl/actief-in-de-kerk/besturen/kerkenraad/privacy

CHECKLIST AVG

1. Check welke gegevens er worden gebruikt en worden opgeslagen in uw gemeente, hoe en waarom ze gebruikt worden en met wie de informatie wordt gedeeld of voor wie de informatie op welke manier toegankelijk is.
2. Check hoe de informatie wordt opgeslagen en hoe deze beschermd is.
3. Bekijk alle processen in uw gemeente waarbij persoonsgegevens een rol spelen en of deze gerechtvaardigd zijn en volledig gedocumenteerd.
4. Bekijk alle gegevens of er expliciete toestemming is (als dit nodig is) en hoe deze is verkregen en of deze gedocumenteerd is.
5. Bekijk alle procedures met betrekking tot vragen van personen. Zijn deze adequaat en actueel? Kunnen mensen makkelijk hun vraag kwijt?
6. Wat is de procedure voor het actueel houden van de gegevens, wat is de procedure om niet meer noodzakelijke gegevens te verwijderen?
7. Check al de in gebruik zijnde IT systemen op het verwerken van gegevens, de veiligheidsprocedures etc.
8. Maak een soort Data Protection Impact Assessment, het is niet verplicht maar wel goed om te doen. Het is een beoordeling of alle procedures om te voldoen aan regelgeving zijn gedaan (compliance, zie format auditformulier).
9. Indien er sprake is van externe gegevens verwerking of bewerking, dus door derde partijen, stel dan een verwerkings- of bewerkersovereenkomst op.
10. Kijk naar uw huidige beleid voor het melden van datalekken en pas het zo nodig aan. Let hierbij ook op hoeveel computers bepaalde bestanden staan, en hoe hier mee wordt omgegaan. Beperk dit zo mogelijk. Informeer gebruikers in uw gemeente over hun verantwoordelijkheid.

AUDIT formulier

Voor alle bestanden, mail lijsten, spreadsheets, papieren documentem en andere persoonsgegevens.

Omschrijving	Waarom data bewaren, waarvoor gebruikt?	Basis. Toestemmin nodig?	Wie beschikt over data, wie heeft toegang?	Welke veiligheids procedures zijn er?	Hoe lang worden gegevens bewaard?	Past dit binnen AVG?	Welke actie om het aan te passen?

Bron: www.kerkrentmeester.nl Skinversie 1: 22-4-2018

SKIN-Rotterdam SKIN-Rotterdam, gevestigd aan Hang 10, 3011 GG Rotterdam, is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze

privacyverklaring. Contactgegevens: www.skinrotterdam.nl Hang 10, 3011 GG Rotterdam +31102140504

Karin de Schipper is de Functionaris Gegevensbescherming van SKIN-Rotterdam Hij/zij is te bereiken via info@skinrotterdam.nl Persoonsgegevens die

wij verwerken

SKIN-Rotterdam verwerkt uw persoonsgegevens doordat u gebruik maakt van onze diensten en/of omdat u deze zelf aan ons verstrekt. Hieronder vindt u een overzicht van de persoonsgegevens die wij verwerken:

- Voor- en achternaam
- Geslacht
- Adresgegevens
- Telefoonnummer
- E-mailadres
- Gegevens over uw activiteiten op onze website
- Lijst met contactgegevens van de klant via een app
- Internetbrowser en apparaat type

Bijzondere en/of gevoelige persoonsgegevens die wij verwerken

SKIN-Rotterdam verwerkt de volgende bijzondere en/of gevoelige persoonsgegevens van u:

- ras
- godsdienst of levensovertuiging

Met welk doel en op basis van welke grondslag wij persoonsgegevens verwerken

SKIN-Rotterdam verwerkt uw persoonsgegevens voor de volgende doelen:

- Het afhandelen van uw betaling
- Verzenden van onze nieuwsbrief en/of reclamefolder
- U te kunnen bellen of e-mailen indien dit nodig is om onze dienstverlening uit te kunnen voeren
- U te informeren over wijzigingen van onze diensten en producten
- Om goederen en diensten bij u af te leveren
- SKIN-Rotterdam analyseert uw gedrag op de website om daarmee de website te verbeteren en het aanbod van producten en diensten af te stemmen op uw voorkeuren.

Geautomatiseerde besluitvorming

SKIN-Rotterdam neemt [wel / niet] op basis van geautomatiseerde verwerkingen besluiten over zaken die (aanzienlijke) gevolgen kunnen hebben voor personen. Het gaat hier om besluiten die worden genomen door computerprogramma's of -systemen, zonder dat daar een mens (bijvoorbeeld een medewerker van SKIN-Rotterdam) tussen zit. SKIN-Rotterdam gebruikt de volgende computerprogramma's of -systemen: [aanvullen met naam van het systeem, waarom het gebruikt wordt, onderliggende logica, belang en verwachte gevolgen voor betrokkene]

Hoe lang we persoonsgegevens bewaren

SKIN-Rotterdam bewaart uw persoonsgegevens niet langer dan strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld. Wij hanteren de volgende bewaartermijnen voor de volgende (categorieën) van persoonsgegevens: (Categorie) persoonsgegevens > Bewaartermijn > Reden Personalia > Bewaartermijn > Reden Adres > Bewaartermijn > Reden Enzovoort > Bewaartermijn > Reden

Delen van persoonsgegevens met derden

SKIN-Rotterdam verkoopt uw gegevens niet aan derden en verstrekt deze uitsluitend indien dit nodig is voor de uitvoering van onze overeenkomst met u of om te voldoen aan een wettelijke verplichting. Met bedrijven die uw gegevens verwerken in onze opdracht, sluiten wij een bewerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. SKIN-Rotterdam blijft verantwoordelijk voor deze verwerkingen.

Cookies, of vergelijkbare technieken, die wij gebruiken

SKIN-Rotterdam gebruikt alleen technische en functionele cookies. En analytische cookies die geen inbreuk maken op uw privacy. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan deze website wordt opgeslagen op uw computer, tablet of smartphone. De cookies die wij gebruiken zijn noodzakelijk voor de technische werking van de website en uw gebruiksgemak. Ze zorgen ervoor dat de website naar behoren werkt en onthouden bijvoorbeeld uw voorkeursinstellingen. Ook kunnen wij hiermee onze

website optimaliseren. U kunt zich afmelden voor cookies door uw internetbrowser zo in te stellen dat deze geen cookies meer opslaat. Daarnaast kunt u ook alle informatie die eerder is opgeslagen via de instellingen van uw browser verwijderen.

Gegevens inzien, aanpassen of verwijderen

U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door SKIN-Rotterdam en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u beschikken in een computerbestand naar u of een ander, door u genoemde organisatie, te sturen. U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar info@skinrotterdam.nl. Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie uw pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van uw privacy. We reageren zo snel mogelijk, maar binnen vier weken, op uw verzoek. SKIN-Rotterdam wil u er tevens op wijzen dat u de mogelijkheid heeft om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Dat kan via de volgende link: https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons Hoe wij persoonsgegevens beveiligen

SKIN-Rotterdam neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op met onze klantenservice of via info@skinrotterdam.nl

DATA PROTECTION REQUIREMENTS FOR CHURCHES AND CHRISTIAN ORGANISATIONS

A new, Europe-wide, regulation comes into force next year. The implications for churches which hold and process personal data are far reaching. As Christians, we should want to set an example in our performance in this area. **Neil Walker** provides an overview and a call to action. He is an IT educator by profession, was involved in IT training and processes in a large bank, and serves on the boards of Partnership and Church Growth Trust. He is a leader of Caldmore Evangelical Church, Walsall.

25 May 2018 is a key date for the diaries of all church leaders. This is the date chosen for the EU's General Data Protection Regulation[1] (GDPR) to come into force. GDPR is a comprehensive regulation, enacted in 2016, which will strengthen and unify data protection for individuals across Europe. Brexit will have no immediate effect on the applicability of GDPR in the United Kingdom. It will be in force until the UK enacts Brexit legislation repealing or replacing it or incorporating it into UK law at the point the UK leaves the EU, and, given the political sensitivity of the matter, it can be assumed that Brexit legislation will in fact substantially transpose GDPR into UK law.

GDPR in effect adds to or supersedes existing legislation on data protection, which up to this point has been provided by the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications Regulations 2003.

DPA is based around 8 principles of good information handling and will be fully replaced by GDPR next year. *Stewardship* produced an excellent guide to data protection law for churches in May 2009, and while this does not currently appear in their list of briefing papers, you may be able to google it to refresh your memory of its content[2].

The world has changed since 1998. Then, only 10% of households had internet connections; Facebook and other social media did not exist; the smart phone was a pipe dream; and the cloud was, almost literally, pie in the sky. GDPR represents a significant enhancement in regulation, designed to better protect us in an environment where personal information can be stored, moved, used and misused with increasing speed and facility.

GDPR extends the scope of the law, the need for accountability, and the transparency required when collecting and processing data on individuals. It applies to any organisation in Europe and extends the definition of personal data to include any data which could be used to identify an individual to whom it relates (the IP address of someone's computer, mobile phone, or other connected device, for example).

GDPR broadly subsumes the eight principles of DPA, but adds an accountability principle. Under GDPR, a requirement to show how an organisation is complying with data protection principles is introduced—for example, documenting how your organisation has arrived at a decision to process data, demonstrating that policies and training are in place, and showing that auditing of data

[1] EU legislation can be applied in a member state in one of two ways: (1) by a Regulation, which applies directly in all member states from the date it comes into force; or (2) indirectly, where the EU enacts a Directive, the requirements of which then have to be transposed, usually by a deadline specified in the Directive, into the domestic law of each member state so as to achieve the objectives specified by the Directive by means to varying extents at the choice of the member state. GDPR is a Regulation which applies directly. [2] 2
https://www.stewardship.org.uk/downloads/briefingpapers/Guide%20to%20data%20protection%20law%20for%20churches.pdf

processing is carried out. Organisations must determine and document the legal basis for processing personal data. Privacy must be built into the design of processes for holding and handling data—not collecting anything that is not required, not holding it for longer than required for operational purposes, and ensuring that storage and transmission is secure.

GDPR strengthens the need for organisations to be transparent in their data processing. Privacy notices need to specify the legal basis for processing the data, data retention periods, and contact details for complaints. This is in addition to the existing rules which cover identity of the organisation and intended use of data. Each individual (referred to in the jargon as the 'data subject') needs to be appraised of their right to:

- see what data are held about them (subject access); this must be granted free of charge
- have inaccuracies in any data held about them corrected
- have information erased (and forgotten by the organisation)
- prevent direct marketing to them by the organisation
- data portability (to be provided with an electronic copy of the data relevant to them)

The legal basis for processing data is premised on one or more of six conditions:

- consent of the data subject
- performance of any contract with the data subject relating to it
- compliance with a legal obligation
- that the vital interests of the data subject are protected
- that the data acquired and held is needed for the performance of a task carried out by the organisation in the public interest
- that the legitimate interests of data subjects are protected

Where consent is used as the legal basis for data processing, this is not simply a general, or implied consent. It must be by an unambiguous positive indication of wish in a statement or by clear affirmative action. This means specific and explicit consent for each processing activity, evidenced and auditable, dynamic (not open-ended), and easy to withdraw. In practice, this means that, in every instance where you collect and process data electronically, there is a need to record the opt-in action of each data subject, not simply with a tick box, but with a record that indicates when the subject agreed, and what they were agreeing to. They must also be made aware of the process by which they can withdraw their consent on an ongoing basis.

GDPR introduces special protection for children's personal data. Broadly, for a child under 13 there will be a need to have consent from a parent or guardian in order to process any data lawfully.

GDPR mandates identification and notification of breaches of the regulation to the individual, and sometimes the national regulator (the Information Commissioner's Office, ICO) within 72 hours. The maximum fine for organisations which breach the regulation will be €20 million. Quite apart from anything else, this should give charity trustees pause for thought.

GDPR may require the appointment of a Data Protection Officer in some circumstances, but in all circumstances there will be a need to ensure that someone in the organisation has been designated as responsible for data protection, and that they have the necessary knowledge, support and authority to ensure that the organisation is applying the regulation effectively.

All of this protection should be comforting to us as data subjects—in principle, we can look forward to freedom from unsolicited begging letters, from unwanted direct mailing, from web sites capturing

our data for unknown purposes. But the regulation brings additional responsibilities on us as church leaders, and the nature of our response before a watching world is important.

In the past, some of us may have taken mental cover from the requirements of the DPA, by saying to ourselves that we are too small an organisation for the authorities to be worried about, or perhaps that we don't really process any data—we just have an address book, an attendees list, a prayer list. Indeed, there was an exemption from registration with ICO for churches which solely held and processed:

- Church membership list (where individuals have provided their details themselves)
- Gift Aid records
- Accounting records
- Payroll records

Under GDPR, this is not a sustainable response and, in any case, churches and other organisations may well have been breaching the current legislation. ICO has already signalled that it intends to enforce the law, having already fined 13 charities, some relatively small, for improper use of data so far this year. Elizabeth Denham, the Commissioner, has been quoted as saying: 'These fines draw a line under what has been a complex investigation into the way some charities have handled personal information. While we will continue to educate and support charities, we have been clear that what we now want, and expect, is for charities to follow the law.' The regulation demands that, even for small churches, our electronic collection and use of personal data is thought about, managed, and tested in advance.

Let's take the case of the organisation of a Children's Holiday Club. Consents will be required for children to attend, lists generated for group leaders, and contact details stored and made available as necessary. Sensitive data, including medical conditions, allergies, parental access restrictions, etc., will be required to ensure that helpers can make properly informed decisions during club activities. In the past, these are organisational details that church Leaders would just cope with—perhaps drop in a box file and pull out again next summer?

From May 2018, there will be a mandated need to plan in advance the basis on which this data is to be collected, stored, processed and retained. Will leaders be sent group details on their personal smart phones? If so, how will access be controlled? What will be the retention policy for that data? How will the parent/guardian verify what is being held? How will they make contact to demand removal of data? How can they be provided with electronic copy for data portability? This is the way of the world in which we are called to be witnesses and we must respond in a way which is generous, open hearted, and at the very least abides by the new law.

Other common scenarios come to mind—addresses and birth dates of those who have attended ladies meetings, 'down the shed' clubs and other neighbourhood outreach are often held to enable us to send birthday cards, invitations, newsletters, calendars. This is data storage and processing and is subject to GDPR. Simply storing membership and prayer lists in electronic form brings these items under regulation. Just a couple of minutes spent mentally reviewing the activities of your church will probably generate a number of instances for your particular situation.

In relation to direct marketing, which both the existing law and GDPR also regulates, it is tempting to rely on the idea that this only applies where someone is selling something, or soliciting money. Church leaders need to be aware that in law this term applies more broadly, and covers the promotion of aims and ideals as well as any advertising or marketing communication (whether trying

to sell a product or promoting an organisation) that is directed to particular individuals. Think about the impact for texts and emails containing invitations to events, promotion of camps, church weekends, requests for support of needy causes, etc., or indeed simply church newsletters. Specific consent needs to have been sought and obtained from each recipient, even from existing contacts and supporters, before such texts and emails are issued by an organisation.
One short article in Perspectives is not going to provide a solution, but we have 9 months now in which to prepare, and a number of organisations are providing advice and guidance. ICO (ico.org.uk) has a web site section specifically for small charities, with readable guides and downloadable tools to support your preparation. ICOs top five tips for you are:

Tell people what you are doing with their data.
People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice), so it is important you are open and honest with people about how their data will be used.

Make sure your staff/volunteers are adequately trained
New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff and volunteers.

Use strong passwords
There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves. Passwords should not be disclosed to others, even within the organisation.

Encrypt all portable devices
Make sure all portable devices—such as memory sticks and laptops— used to store personal information are encrypted.

Only keep people's information for as long as necessary
Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

Microsoft has committed to supporting its customers by ensuring that Windows 10, Office 365, and its Cloud services are completely GDPR compliant by May 2018. *Dropbox* is committed to the security and the protection of users' data in line with legal requirements and best practices at all times. It is also committed to enhancing its systems as further guidance emerges, so that it meets or exceeds legal requirements going forward.

The tools we use to handle data in the modern age will be ready. We must be too.
We would encourage you to make best use of the preparation time using four simple steps:

1. Discover
Identify what personal data you have and where it resides
2. Manage
Govern how personal data is used and accessed, in line with the legal requirements **3. Protect**

Establish security controls to prevent, detect and respond to vulnerabilities and data breaches **4. Report**
Keep required documentation, manage data requests and breach notifications

The Apostle Paul, in his letter to Titus, urges him to remind God's people to be subject to rulers and authorities, to be considerate, to be ever ready to do what is good. Let's glorify God as we make preparations for May 2018.

ACTION NEEDED

THE CHURCH OF ENGLAND

GDPR CHECKLIST

The General Data Protection Regulation (GDPR) will take effect in the UK in May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations. Parishes must comply with its requirements, just like any other charity or organisation. Use this handy checklist to make sure you're on top of what you need to do. See also our guidance at *www.parishresources.org.uk/gdpr*

The Checklist	*Sorted*	*Action needed & date completed*
1 **Data Audit** Use our template to review your data processing. This is a great first step to identify the other action you will need to take. We've provided a template at *www.parishresources.org.uk/gdpr/dataaudit*	☐	
2 **Privacy Notice:** Have you drafted a Privacy Notice. You can find guidance and a sample template at: *www.parishresources.org.uk/gdpr/privacy* Is it available online for people to access? Is there a date set to review it?	☐ ☐ ☐	
3 **Do you need to get additional consent….** It's likely that many parishes will need to get additional consent from people as either consent has been assumed, or the evidence of the consent is no longer available. See our example consent forms at *www.parishresources.org.uk/gdpr/consent*	☐	
4 **Are your procedures up to date?** Data subjects (those people about whom you hold personal data) have the right to see what data is being stored about them, to make corrections where there are errors, or to ask for their data to be deleted. Do you have processes in place to meet such requests?	☐	

5 What if you had a breach

Review your breach management procedures and ensure that you know what to do in the event of a breach. If you don't have any, you will need to develop them. See our guide at *www.parishresources.org.uk/gdpr*

EXAMPLE – for illustrative purposes only. This will not be applicable in every Parish. If you wish to reapply this, you will need to replace the PCC name with your own throughout the document and put in relevant contact details in the highlighted place in Section 9.

DATA PRIVACY NOTICE

The Parochial Church Council (PCC) of St Agatha's, Anytown

1. Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

2. Who are we?

The PCC of St Agatha's, Anytown is the data controller (contact details below). This means it decides how your personal data is processed and for what purposes.

3. How do we process your personal data?

The PCC of St Agatha's, Anytown complies with its obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
- To administer membership records;
- To fundraise and promote the interests of the charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records (including the processing of gift aid applications);
- To inform you of news, events, activities and services running at St Agatha's;
- To share your contact details with the Diocesan office so they can keep you informed about news in the diocese and events, activities and services that will be occurring in the diocese and in which you may be interested.

4. What is the legal basis for processing your personal data?

- Explicit consent of the data subject so that we can keep you informed about news, events, activities and services and keep you informed about diocesan events.
- Processing is necessary for carrying out legal obligations in relation to Gift Aid or under employment, social security or social protection law, or a collective agreement;

- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided: - ○ the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
    ○ there is no disclosure to a third party without consent.

5. Sharing your personal data

Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out a service to other church members or for purposes connected with the church. We will only share your data with third parties outside of the parish with your consent.

6. How long do we keep your personal data[1]?

We keep data in accordance with the guidance set out in the guide "Keep or Bin: Care of Your Parish Records" which is available from the Church of England website [see footnote for link].

Specifically, we retain electoral roll data while it is still current; gift aid declarations and associated paperwork for up to 6 years after the calendar year to which they relate; and parish registers (baptisms, marriages, funerals) permanently.

7. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the PCC of St Agatha's, Anytown holds about you;
- The right to request that the PCC of St Agatha's, Anytown corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for the PCC of St Agatha's, Anytown to retain such data;
- The right to withdraw your consent to the processing at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable) [*Only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and in either case the data controller processes the data by automated means*].
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable) [*Only applies where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics*]

[1] Details about retention periods can currently be found in the Record Management Guides located on the Church of England website at: - https://www.churchofengland.org/more/libraries-and-archives/records-management-guides

- The right to lodge a complaint with the Information Commissioners Office.

8. Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

9. Contact Details

To exercise all relevant rights, queries of complaints please in the first instance contact the PCC Secretary / Parish Administrator at [insert contact details].

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.