HANDLEIDING DATALEKKEN

VOOR R.-K. PAROCHIES

 mei 2019

Inhoud

1. Inleiding

In een parochie werken vrijwilligers en beroepskrachten met persoonsgegevens. Waar mensen werken gaat er wel eens iets mis. Dat geldt ook voor het werken met persoonsgegevens. In deze handleiding leest u wat u dan moet doen.

Wanneer persoonsgegevens kwijtraken of door onbevoegden worden ingezien, wordt dat een datalek genoemd. Het term *datalekken* heeft al snel een negatieve bijklank. Het is goed om dit te doorbreken, want in alle organisaties gaat er wel eens wat fout. Het doel van de wetgever is dat mensen zich van incidenten bewust worden, er transparant over zijn en ervan leren.

Het helpt als vrijwilligers en beroepskrachten in de parochie weten wat ze moeten doen als er een incident plaatsvindt. Een datalek wordt mogelijk erger als er niet gehandeld wordt, terwijl dit wel had gemoeten. Maak het onderwerp daarom bespreekbaar binnen het bestuur, met de werknemers en natuurlijk de vele vrijwilligers binnen de parochie. Gebruik hiervoor bijvoorbeeld de PowerPointpresentatie die beschikbaar is gesteld op www.rkkerk.nl/avg

Om u te informeren over dit onderwerp en om u praktische voorschriften aan te reiken, is deze handleiding opgesteld.

Actiepunt: Werk aan bewustwording. Geef vrijwilligers en beroepskrachten de informatie om met vertrouwen te kunnen werken. [zie: Hoofdstuk 2]

2. Drie basisstappen om incidenten te gaan herkennen

Veel mensen vinden het herkennen van een datalek lastig. Daarom volgen hier drie basisstappen die beroepskrachten en vrijwilligers in de parochie helpen om incidenten te gaan herkennen.

Stap 1 Breng in beeld te welke persoonsgegevens de parochie verwerkt, wie toegang heeft tot deze gegevens en hoe lang deze bewaard blijven. Door de gegevensstroom in beeld te brengen, wordt zichtbaar waar een mogelijk datalek plaatsvindt.

Het herkennen van datalekken is dus de vrucht van een bewustwordingsproces: hoe ga ik met gegevens om en waar maak ik (nog) fouten?

Stap 2 Werk aan bewustwording over datalekken. Dit kan het parochiebestuur doen door met het pastoraal team, werknemers en vrijwilligers te spreken over gegevensbescherming en datalekken. Gebruik hiervoor eventueel de PowerPointpresentatie die beschikbaar is gesteld op www.rkkerk.nl/avg. Nóg belangrijker is dat alle mensen die met persoonsgegevens omgaan, zich bewust zijn van de privacy-gevoeligheid.

Stap 3 Maak in de parochie bekend bij wie medewerkers en vrijwilligers terecht kunnen met vragen en meldingen. Weten de medewerkers en vrijwilligers wat zij moeten doen bij een datalek? Stel in het bestuur het meldingsprotocol [zie: Hoofdstuk 3] vast en maak dit onder de medewerkers en vrijwilligers bekend.

3. Een meldingsprotocol en eerste aanspreekpunt

Medewerkers en vrijwilligers in de parochie moeten weten bij wie zij terecht kunnen als zij een incident constateren. Het parochiebestuur is verantwoordelijk voor het juist handelen bij een incident of datalek. Het parochiebestuur wijst daarom uit zijn midden iemand aan als aanspreekpunt voor het thema datalekken. Uiteraard kan een deskundige vrijwilliger of medewerker het betreffende bestuurslid bijstaan in deze rol. Het bestuur stelt het meldingsprotocol vast [zie: Hoofdstuk 10]. In het meldingsprotocol staat beschreven wie welke verantwoordelijkheden heeft op het moment dat zich een mogelijk datalek voordoet.

Twee of drie mensen weten meer dan één. Het onderzoek naar een mogelijk datalek vindt weliswaar plaats onder de verantwoordelijkheid van het parochiebestuur, maar dat betekent niet dat het bestuur er alleen voor staat. Maak gebruik van deskundige medewerkers en/of vrijwilligers op het gebied van gegevensbescherming.

Actiepunt: Vul het model-meldingsprotocol datalekken in. U vindt het modelmeldingsprotocol in hoofdstuk 10 van deze handleiding. Stel dit protocol vast in het parochiebestuur.

4. Wat is een datalek?

Een datalek is een incident waarbij persoonsgegevens zonder dat dit de bedoelding is:

a) zijn vernietigd (en dus niet meer bestaan);
b) kwijt zijn geraakt (de persoonsgegevens bestaan nog wel, maar je weet niet waar ze zijn en je hebt er dus geen controle meer over. Denk aan diefstal.);
c) zijn openbaargemaakt (bijvoorbeeld doordat ze zijn gepubliceerd);
d) zijn ingezien door onbevoegden (bijvoorbeeld onbevoegde inzage in een personeelsdossier of het doorsturen van een verkeerde bijlage met persoonsgegevens);
e) zijn gewijzigd of bewaard zonder dat dit bedoeling is.

Voorbeelden van mogelijke datalekken:

- U voegt een verkeerd bestand (met hierin persoonsgegevens) bij een e-mail.
- Een vrijwilliger of medewerker krijgt onbevoegd toegang tot persoonsgegevens
  - Iemand ziet onbevoegd een (personeel)dossier in.
- Een laptop of usb-stick raakt verloren, waardoor onbekend is in welke handen de persoonsgegevens vallen.
- Een groepsmail verbergt niet alle e-mailadressen
  - Zijn de leden van de groep er akkoord mee dat hun privé-emailadressen gedeeld worden met anderen? Dan hoeven de persoonsgegevens niet verborgen te worden.
- Ingevulde (aanmeld)formulieren met hierop persoonsgegevens raken kwijt.
- Een gepersonaliseerde brief wordt verzonden aan een verkeerd adres.

5. Wat moet een parochie bij een datalek doen?

Nadat een incident is ontdekt, worden de volgende stappen doorlopen:

Stap 1:	Melding aan het parochiebestuur
Stap 2:	Toets of/welke persoonsgegevens gelekt zijn
Stap 3:	Toets of het incident mogelijke risico's oplevert voor de betrokkene
Stap 4:	Voer de juiste acties uit
Stap 5:	Evalueer het incident en trek lessen voor de toekomst

Stap 1: De melding aan het parochiebestuur

Een medewerker of vrijwilliger signaleert dat er een incident is geweest waarbij mogelijk persoonsgegevens kwijtgeraakt, verloren, verkeerd verstuurd, ingezien of gewijzigd zijn. Het incident wordt volgens het meldingsprotocol gemeld bij het verantwoordelijke bestuurslid. Zorg ervoor dat de melding gemakkelijk persoonlijk of telefonisch gemaakt kan worden.

Actiepunt: Zorg ervoor dat het meldingsprotocol bekend en beschikbaar is voor de beroepskrachten en vrijwilligers in de parochie.

Stap 2: Toets of het incident persoonsgegevens betreft

Het parochiebestuur ontvangt de melding. Het bestuurslid stelt vragen om informatie te verzamelen over wat er is gebeurd. Dat zijn de volgende vragen:

a) Breng het tijdpad in beeld. Wanneer is wat gebeurd?
b) Stel vast of er persoonsgegevens zijn: verloren gegaan, openbaar gemaakt, ingezien, gewijzigd of doorgestuurd.
c) Stel vast welke categorie(en) persoonsgegevens bij het incident betrokken zijn (NAW-gegevens, bijzondere persoonsgegevens, financiële gegevens, medische gegevens etc.)

Actiepunt: Duurt het datalek nog voort? Zorg dan voor acute maatregelen.

Drie voorbeelden van incidenten en acute maatregelen:

1. Men constateert dat een telefoon met privé-contactgegevens erin is gestolen.
   Acute maatregel: Laat de simkaart/telefoon blokkeren.
2. Men constateert dat het slot van de archiefkast kapot is waardoor onbevoegden toegang kunnen krijgen (dit is een beveiligingsincident).
   Acute maatregel: Laat het slot maken of plaats een noodslot.
3. Zeer vertrouwelijke gegevens, zoals een personeelsdossier of een VOG, worden op een algemeen toegankelijke plaats gevonden.
   Acute maatregel: Berg de documenten onmiddellijk op een gesloten plaats op.

Stap 3: Toets of het incident mogelijke risico's oplevert voor betrokkenen

Als iemands persoonsgegevens verloren zijn gegaan, kwijt zijn geraakt, openbaar zijn gemaakt, doorgestuurd of gewijzigd kan de betrokkene daar nadeel van ondervinden. Het incident kan voor de betrokkene risico's met zich meebrengen.

Een datalek moet aan de Autoriteit Persoonsgegevens worden gemeld als voor de betrokkene een risico is op:

A. Het verlies van controle over zijn/haar persoonsgegevens;
B. discriminatie;
C. identiteitsdiefstal of -fraude;
D. financiële verliezen;
E. reputatieschade;
F. verlies van vertrouwelijkheid van beschermde persoonsgegevens.

Raadpleeg hoofdstuk 7 voor een toelichting op en praktische voorbeelden van situaties waarin bovengenoemde risico's zich kunnen voordoen. Vraag advies aan de AVG-contactpersoon van uw Bisdom als u vragen heeft over het maken van de juiste afweging.

Actiepunt: Weet op welke risico's u bedacht moet zijn. Dit helpt om snel te kunnen inschatten of een incident risico's heeft voor de betrokkene en of het incident gemeld moet worden bij de Autoriteit Persoonsgegevens.

Stap 4: Voer de juiste acties uit

Het incident is in beeld gebracht. Aan de hand van de informatie weet u welke persoonsgegevens zijn gelekt en of het waarschijnlijk is dat hierdoor risico's ontstaan voor betrokkene(n). Aan de hand van de informatie stelt u vast welke situatie zich voordoet en welke bijbehorende acties moeten worden uitgevoerd.

Overzicht van 'geconstateerde situaties en bijbehorende acties'

Situatie 1: U constateert dat er *geen* sprake is van een datalek, omdat er geen persoonsgegevens verloren zijn gegaan, ingezien, gewijzigd of openbaar gemaakt. U stelt vast dat er een beveiligingsincident heeft plaatsgevonden.

→ Actie: vul het register van incidenten en datalekken in en ga naar stap 5.

Situatie 2: U constateert dat er wel sprake is van een datalek. U stelt vast dat het *niet* waarschijnlijk is dat het datalek een risico oplevert voor de betrokkene(n).

→ Actie: vul het register van incidenten en datalekken in en ga naar stap 5.

Situatie 3: U constateert dat er sprake is van een datalek en dat dit waarschijnlijk een risico oplevert voor betrokkene(n).

→ Actie: Start de procedure om het datalek binnen 72 uur na ontdekking te melden bij de Autoriteit Persoonsgegevens. Informeer zowel de pastoor als de AVG-contactpersoon van het Bisdom over uw voornemen. Onderzoek of het datalek ook gemeld moet worden aan de betrokkene. Ga daarna naar stap 5.

Situatie 4: Er is sprake van een datalek met risico voor de betrokkene(n) en het is zeer waarschijnlijk dat de betrokkene(n) hiervan last gaat/gaan ondervinden.

→ Actie: Zorg dat er binnen 72 uur nadat het datalek is ontdekt een (voorlopige) melding bij de Autoriteit Persoonsgegevens wordt gedaan en informeer de betrokkene(n) over het incident. Ga daarna naar stap 5.

Stap 5: Evalueer het incident en neem preventieve maatregelen

Naar aanleiding van het datalek heeft het parochiebestuur de acties ondernomen die horen bij de ernst van het datalek. Naar aanleiding van deze acties zijn er nog drie belangrijke taken:

Drie taken nadat het incident heeft plaatsgevonden:

1. **Vul het register in:** Het verantwoordelijke bestuurslid vult het register van incidenten en datalekken zo volledig mogelijk in;

- **Evalueer het incident:** Evalueer met de betrokken bestuursleden, beroepskrachten en vrijwilligers wat er is gebeurd en welke les er wordt getrokken om het incident in de toekomst te voorkomen;

  Tip: Creëer geen straffende sfeer of angstcultuur. Wees open in het gesprek en leer van elkaar.

2. **Tref preventieve maatregelen:** Om dit soort incidenten te voorkomen kunt u regels onder de aandacht brengen, verduidelijken, aanpassen of nieuwe veiligheidsmaatregelen nemen. Spreek tijdens de evaluatie af wie verantwoordelijk is voor het uitvoeren van de vervolgstappen.

6. Het bijhouden van een register van datalekken en beveiligingsincidenten

Het model-register

In een register van datalekken en beveiligingsincidenten houdt het parochiebestuur bij welke incidenten hebben plaatsgevonden en welke acties zij hierop heeft ondernomen. Het bijhouden van het register is een wettelijke plicht. Op www.rkkerk.nl/avg is een model-register beschikbaar gesteld.

Wie moet het register bijhouden?

Het parochiebestuur is verantwoordelijk voor het bijhouden van het register. Het parochiebestuur kan zich laten bijstaan door een of twee medewerkers of vrijwilligers die thuis zijn in dit onderwerp (zie: Hoofdstuk 2)

Wat moet er in het register vastgelegd worden?

Voor parochies en andere kerkelijke instellingen is er een model-register van datalekken en incidenten beschikbaar op www.rkkerk.nl/avg. Dit model-register geeft een overzicht van alle informatie die u verplicht moet registreren.

7. Moet een incident bij de Autoriteit Persoonsgegevens worden gemeld?

Wie is verantwoordelijk voor de melding?

Als er een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens dan gebeurt dit altijd onder verantwoordelijkheid van de pastoor en het parochiebestuur. Informeer en betrek daarom altijd de pastoor van de parochie bij het voornemen een melding bij de Autoriteit Persoonsgegevens te doen. Informeer ook de AVG-contactpersoon van uw Bisdom over uw voornemen om een melding te doen.

Wanneer moet een incident bij de Autoriteit Persoonsgegevens worden gemeld?

Er volgt een melding bij de Autoriteit Persoonsgegevens als er sprake is van een datalek dat waarschijnlijk een van de onderstaande risico's voor de betrokkene tot gevolg heeft:

Voorbeelden van risico's voor betrokkenen:

a) Door het datalek loopt de betrokkene(n) een aanzienlijk risico de **controle over zijn of haar persoonsgegevens te verliezen**.
Voorbeeld: Dit is bijvoorbeeld het geval als inloggegevens en/of wachtwoorden zijn gelekt.

b) Door het datalek loopt de betrokkene een aanzienlijk risico op **discriminatie of reputatieschade.**
Voorbeeld: Er is een USB-stick verloren. Hierop staan de notulen van een vergadering met vertrouwelijk informatie over iemand.
NB: of er risico is op discriminatie of reputatieschade is altijd afhankelijk van de vraag welke persoonsgegevens precies zijn gelekt.

c) Door het datalek loopt/lopen de betrokkene(n) het risico op **identiteitsdiefstal of –fraude.**
Voorbeeld: Er is een personeelsdossier kwijt met daarin een kopie van een legitimatiebewijs en/of vermelding van het Burgerservicenummer (BSN).

d) Door het datalek loopt/lopen de betrokkene(n) het risico op **financiële verliezen.**
Voorbeeld: Machtigingenformulier voor Actie Kerkbalans worden doorgestuurd naar een onbevoegd persoon.

e) Risico op openbaar maken van gegevens die vallen onder een **beroepsgeheim.**
Voorbeeld: medische gegevens of een VOG wordt door onbevoegden ingezien.

Conclusie: Loopt de betrokkene door het incident één van de bovengenoemde risico's of kunt u dat niet uitsluiten? Informeer dan de pastoor van de parochie en de AVG-contactpersoon van uw bisdom over de situatie en meld het incident bij de Autoriteit Persoonsgegevens.

8. Hoe maakt de parochie een melding bij de Autoriteit Persoonsgegevens?

De Autoriteit Persoonsgegevens moet binnen 72 uur nadat het datalek is ontdekt een melding ontvangen. De meldingstermijn van 72 uur laat zien hoe belangrijk het is dat het bestuurslid dat als contactpersoon optreedt, snel wordt geïnformeerd. Zorg er daarom voor dat medewerkers en vrijwilligers bekend zijn met het meldingsprotocol.

Heeft het parochiebestuur geconstateerd dat er sprake is van een datalek met waarschijnlijk risico's voor de betrokkene(n), maar zijn nog niet alle feiten helder? Dan is het raadzaam om binnen 72 uur een voorlopige melding te doen. De parochie heeft de mogelijkheid een melding later aan te vullen of in te trekken. Wacht niet te lang met het aanvullen van een voorlopige melding en doe die dus binnen enkele dagen.

Het is belangrijk dat de parochie het meldingsformulier zo volledig mogelijk invult. Geef duidelijk aan wat er is gebeurd en wees volledig. Een melding bij de Autoriteit Persoonsgegevens wordt digitaal gedaan via onderstaand formulier:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Hoe gaat de Autoriteit Persoonsgegevens met meldingen om?

De Autoriteit Persoonsgegevens doet geen uitspraken aan derden over individuele meldingen van datalekken. Als de parochie een datalek bij de Autoriteit Persoonsgegevens meldt, dan maakt de Autoriteit Persoonsgegevens dus niet de naam van de parochie bekend. De Autoriteit Persoonsgegevens maakt alleen bekend over welke sectoren zij de meeste meldingen ontvangt.

9. Moet de betrokkene over het datalek worden geïnformeerd?

De parochie moet de betrokkene(n) over het datalek informeren als het risico groot is dat het datalek voor de betrokkene(n) zal leiden tot discriminatie, (identiteits-)fraude, financiële schade en/of reputatieschade van de betrokkene(n).

Oplopende nadelige gevolgen voor de betrokkene kunnen soms worden voorkomen:

- Als er in uw bestanden maatregelen zijn getroffen, waardoor de gelekte persoonsgegevens onbegrijpelijk zijn voor onbevoegden. Bijvoorbeeld doordat de betreffende gegevens goed zijn versleuteld.

  Bijvoorbeeld: een laptop wordt gestolen, maar de informatie op de laptop is volledig versleuteld.

- Als de gelekte persoonsgegevens onmiddellijk na het datalek op afstand zijn gewist, nog voordat de onbevoegde ontvanger iets met de gegevens kon doen.

  Bijvoorbeeld: een mobile telefoon raakt kwijt, maar de gegevens op het toestel zijn op afstand door de provider gewist.

10. MODEL Meldingsprotocol datalekken

Parochie (naam invullen: _____

Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Het kan gaan om een kwijtgeraakte USB-stick of een gestolen laptop met persoonsgegevens, maar ook om een inbraak in een datasysteem of per ongeluk verstrekte toegang tot gegevens aan personen of instanties die daartoe geen toegang zouden mogen hebben.

Als sprake is van een ernstig datalek dan zijn de pastoor en het parochiebestuur op grond van de Algemene verordening gegevensbescherming (AVG) verplicht om dit te melden aan de Autoriteit Persoonsgegevens en soms ook aan de betrokkene(n). Als een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens moet dit binnen 72 uur na de ontdekking van het datalek plaatsvinden.

Om er voor te zorgen dat incidenten tijdig worden gemeld, lopen de meldingen centraal via het parochiebestuur. Wie het eerste aanspeekpunt leest u in dit meldingsprotocol. Bij een mogelijk datalek neemt u met deze persoon contact op. Dit bestuurslid vormt, eventueel samen met andere personen, het meldpunt datalekken en beslist wat de volgende stap is.

Het meldpunt datalekken

Een incident of datalek kan door medewerkers en vrijwilligers van de parochie worden doorgegeven aan:

[Naam + e-mailadres + verantwoordelijke namens het parochiebestuur van de parochie]

Onder verantwoordelijkheid van het parochiebestuur vormen de onderstaande personen de leden van het meldpunt datalekken:

- [naam van de persoon die eventueel samen met voornoemde bestuurder het meldpunt datalekken vormt]
- [naam van de persoon die eventueel samen met voornoemde bestuurder het meldpunt datalekken vormt]

Het protocol

1.1 Onmiddellijk nadat een werknemer/vrijwilliger ontdekt of ter ore komt dat er sprake kan zijn van een datalek binnen de parochie, meldt hij/zij dat bij de bovengenoemde verantwoordelijke namens het parochiebestuur. Als de verantwoordelijke namens het parochiebestuur niet bereikbaar is, kan de melding worden gedaan bij de andere personen van het meldpunt datalekken.

1.2 De verantwoordelijke namens het parochiebestuur schakelt het meldpunt datalekken in. Zij beslissen als team of er sprake is van een (mogelijk) datalek en zo ja, of dit datalek moet worden gemeld bij de Autoriteit Persoonsgegevens en/of bij de betrokkene(n).

1.3 Een lid van het meldpunt datalekken kan advies vragen bij de AVG-contactpersoon van het bisdom. Dit is in het bisdom persoon: [NN] De AVG-contactpersoon kan middels de vragen uit

het modelregister voor datalekken en incidenten adviseren of u alle informatie heeft verzameld om de juiste vervolgstappen te nemen.

1.4 Als er een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens dan gebeurt dit altijd onder verantwoordelijkheid van het parochiebestuur. Infomeer daarom altijd de pastoor over uw voornemen om een melding bij de Autoriteit Persoonsgegevens te doen. Informeer ook de AVG-contactpersoon van uw Bisdom over uw voornemen om een melding te doen.

1.5 Het meldpunt datalekken draagt zo nodig zorg voor de melding aan de Autoriteit Persoonsgegevens en/of de betrokkene(n). Het is de werknemer of vrijwilliger niet toegestaan om het (mogelijke) datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) te melden.

1.6 Het meldpunt datalekken draag er zorg voor dat alle incidenten en/of datalekken worden geregistreerd in het register van datalekken en dat de uitkomst wordt geëvalueerd.