VERENIGING VOOR KERKRENTMEESTERLIJK BEHEER IN DE PKN

Databeheer in de kerk

Het principe

Per 1 januari 2016 is de Wet Datalekken (…) van kracht. Organisaties die persoonsgegevens verwerken zijn verplicht om inbreuken op de beveiliging te melden. Het gaat dan binvoorbeeld om diefstal, verlies of misbruik van persoonsgegevend. Doel van de meldplicht is om tot een betere bescherming van de persoonsgegevens te komen. Als je zo'n datalek niet meldt, kunnen er hoge boetes opgelegd worden.

De regels van de Wet Datalekken zijn verwerkt in de Wet Bescherming Persoonsgegevens (WBP). Daarin staat nu de dat de verantwoordelijke partij verplichtingen moet nakomen in verband met een inbreuk op de beveiliging van persoonsgegevens. De kans dat er een nadelig gevolg kan voor de bescherming van persoonsgegevens mag niet optreden. Wie persoonsgegevens beheert of verwerkt is daarvoor verantwoordelijk.

Per 25 mei 2018 gaat de Algemene Verordening Gegevensbescherming (AVG) gelden. Er is dan nog maar één privacywet in de hele EU. Nu hebben de lidstaten nog hun eigen nationale wetten, gebaseerd op de Europese privacyrichtlijn uit 1995. Zodra de algemene verordening gegevensbescherming (AVG) van toepassing is, kunnen organisaties verplicht zijn een functionaris voor de gegevensbescherming (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Op grond van artikel 37 van de AVG is een FG in drie situaties verplicht.

Wat is een datalek?

Belangrijke vraag is natuurlijk wat een datalek precies is. Het gaat om een situatie dat persoonsgegevens verloren raken of dat ze onrechtmatig worden verwerkt. Dat is dus vrij breed. We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsprobleem. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen geprinte klantenlijst evengoed een datalek vormen.

Andere voorbeelden: cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks.

Illegaal verkregen bedrijfsgegevens over een productieproces of marktstrategie betreffen kostbare informatie, maar vallen niet onder de gangbare definitie van datalek.

Als een bedrijfstelefoon verloren of gestolen wordt, dan is dat mogelijk een datalek. Als een privé-telefoon kwijtraakt is er geen datalek (de WBP is niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend persoonlijke of huishoudelijke doeleinden).

Brede Meldplicht datalekken

Sinds 2011 bestaat er een meldplicht voor aanbieders van openbare elektronische communicatiediensten van inbreuken op de beveiliging van persoonsgegevens. Dist ie nog op bass van de telecommunicatiewet.

Datalekken op grond van deze zogenaamde *smalle meldplicht* moeten sinds 1 januari 2016 worden gemeld bij de Autoriteit Persoonsgegevens. De bijbehorende boetes wijken af van de boetes die gelden bij een overtreding van de Wbp.

De algemene meldplicht datalekken voor bedrijven en overheid wordt ook de *brede meldplicht* genoemd. Deze meldplicht werd opgenomen in een nieuw artikel in de Wet Bescherming Persoonsgegevens (WBP) (artikel 34 a). De klemtoon bij deze meldplicht ligt op het lekken van persoonsgegevens als gevolg van beveiligingsproblemen. Deze datalekken moeten - als ze voldoende ernstig zijn - onverwijld worden gemeld aan de toezichthouder, de Autoriteit Persoonsgegevens (AP). De AP is de overheidsinstantie die toeziet op een zorgvuldig gebruik van persoonsgegevens. Nederland loopt met de Wet Meldplicht Datalekken vooruit op de Algemene Verordening Gegevensbescherming waarin ongeveer dezelfde bepalingen zijn opgenomen, die dus in 2018 van kracht wordt in de gehele EU.

Wanneer melden als kerk?

Als je als kerk een datalek constateert, dan hoef je dat alleen te melden als het on een 'ernstig' datalek gaat. Dat moet dus gemeld worden aan de AP. Op de site van de AP is een standaardformulier te vinden waarmee dat kan. Onder omstandigheden moet je het ook melden aan de mensen van wie persoonsgegevens gelekt zijn. Het begrip 'ernstig' is nietr afgebakend. Het kan zien op twee kanten. Gaat het om een 'kwalitatief' ernstig lek: er is echt gevoelige informatie kwijt. Of gaat het om een 'kwantitatief' ernstig lek: is er veel tegelijk op straat komen te liggen?

Inhoud van de melding aan de AP over een datalek

Een datalek moet binnen 72 uur gemeld worden bij de toezichthouder. Deze termijn is gerekend vanaf het eerste moment dat het probleem gesignaleerd is, niet het tijdstip van bijvoorbeeld rapportage aan een verantwoordelijke of de juridische afdeling.
De melding aan de toezichthouder omvat in elk geval:

- de aard van de inbreuk;
- de instanties waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
- de maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.

Verwijzingen:

- https://autoriteitpersoonsgegevens.nl/
- https://nl.wikipedia.org/wiki/Autoriteit_Persoonsgegevens
- http://www.justitia.nl/privacy/datalekken.html

De Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) is een zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens. De organisatie houdt zich dus bezig met privacy. De taken van de AP vloeien voort uit de Europese Privacyrichtlijn 95/46/EG die voor alle landen van de EU geldt. Deze richtlijn wordt dus vervangen door de algemene verordening gegevensbescherming. Alle lidstaten van de EU hebben een eigen instantie, soortgelijk aan de AP.

De Autoriteit Persoonsgegevens heeft als wettelijke taak te beoordelen of personen en organisaties de Wet bescherming persoonsgegevens naleven. Deze taak is ook gericht op de overheid. Ook ziet de AP toe op naleving van de Wet politiegegevens, de Wet gemeentelijke basisadministratie persoonsgegevens en alle andere wettelijke regelingen waarin sprake is van het verwerken van persoonsgegevens.

De organisatie heette tot 2016 het College bescherming persoonsgegevens (CBP). Dit college volgde in 2001 de Registratiekamer op. Met de naamswijziging per 1 januari 2016 kreeg het orgaan onder meer de bevoegdheid om boetes op te leggen bij overtredingen van de Wet bescherming persoonsgegevens (WBP). Deze wijzigingen waren een gevolg van ingrijpende aanpassingen in die wet.[1] De naamswijziging van 2016 geldt overigens alleen 'in het maatschappelijk verkeer', zo bepaalt artikel 51 van de WBP. Dat artikel geeft 'College bescherming persoonsgegevens' nog steeds als formele naam aan.

In het kort komt de Wet bescherming persoonsgegevens erop neer dat een organisatie slechts díe persoonsgegevens mag verwerken die voor de organisatie aantoonbaar noodzakelijk zijn en waar geen expliciet verbod voor bestaat . Voorbeelden hiervan zijn medische, seksuele, politieke gegevens en gegevens over het lidmaatschap van een vakbond. Voor overheden betekent de term 'aantoonbaar noodzakelijk' dat er een wettelijke grondslag moet zijn voor het verwerken van deze gegevens.

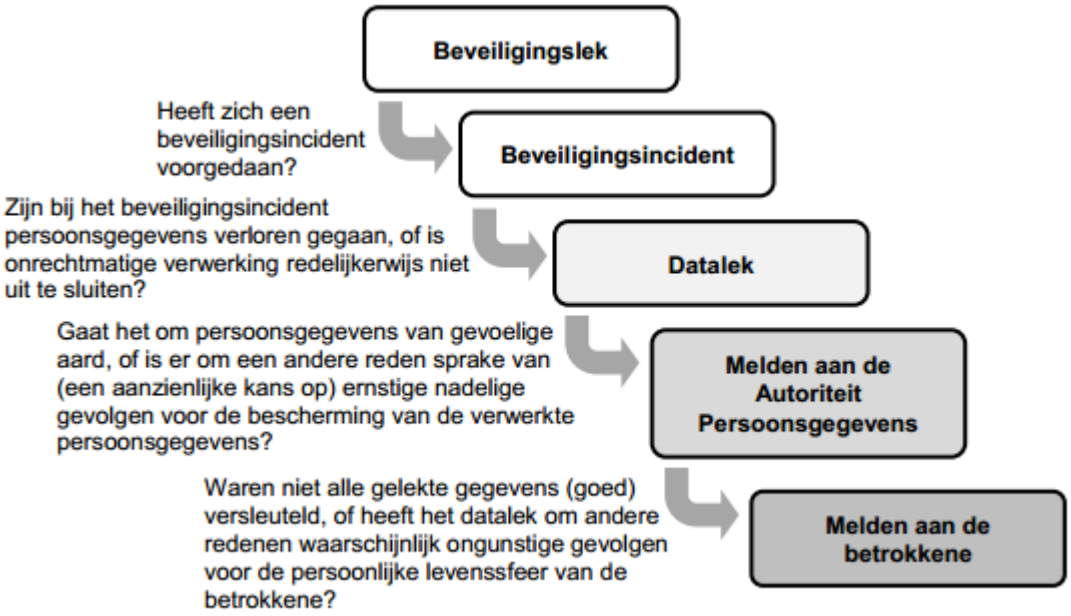
Persoonsgegevens zijn alle gegevens die op welke wijze dan ook zijn te relateren aan een identificeerbare persoon, die bovendien nog in leven moet zijn. Ook telefoonnummers en IP-adressen kunnen persoonsgegevens zijn, zelfs als er niets anders vastgelegd is.

Bijzonder aan de Wet bescherming persoonsgegevens is dat niet wordt uitgegaan van het 'bezit' - eigendom of beheren van gegevens - maar van het gebruik ervan, het 'verwerken'. Met 'verwerken' wordt bedoeld alle handelingen, van registreren en opslaan van de gegevens, tot bewerken, kopiëren, wijzigen, aanvullen en wissen. Als partij A de adresbestanden van B gebruikt voor het versturen van bijvoorbeeld spam, dan valt partij A onder de regels van deze wet.

De toezichthoudende functies houden in dat de Autoriteit Persoonsgegevens bedrijven en overheden kan dwingen om zich aan de eisen van de WBP houden. Hiervoor kan de AP dwangsommen opleggen. Verder heeft de AP een openbaar register van gegevensverwerkingen als deze afwijken van de gebruikelijke verwerkingen. Voor het niet registreren van niet vrijgestelde verwerkingen kan de AP een bestuurlijke boete opleggen. In alle gevallen heeft de rechter echter het laatste woord.

Daarnaast heeft de AP de taak om de ministers en de Tweede Kamer gevraagd en ongevraagd te adviseren over wetsvoorstellen, in het licht van de WBP of andere van toepassing zijnde regels.

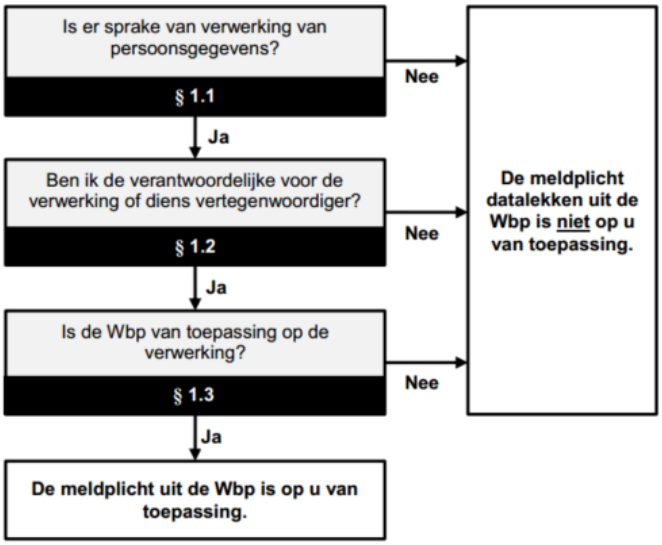
De verplichting tot het melden van datalekken door verantwoordelijken en bewerkers aan de Autoriteit Persoonsgegevens wordt geregeld doordat per 1/1/2016 aanvullende bepalingen opgenomen zijn in de WBP.

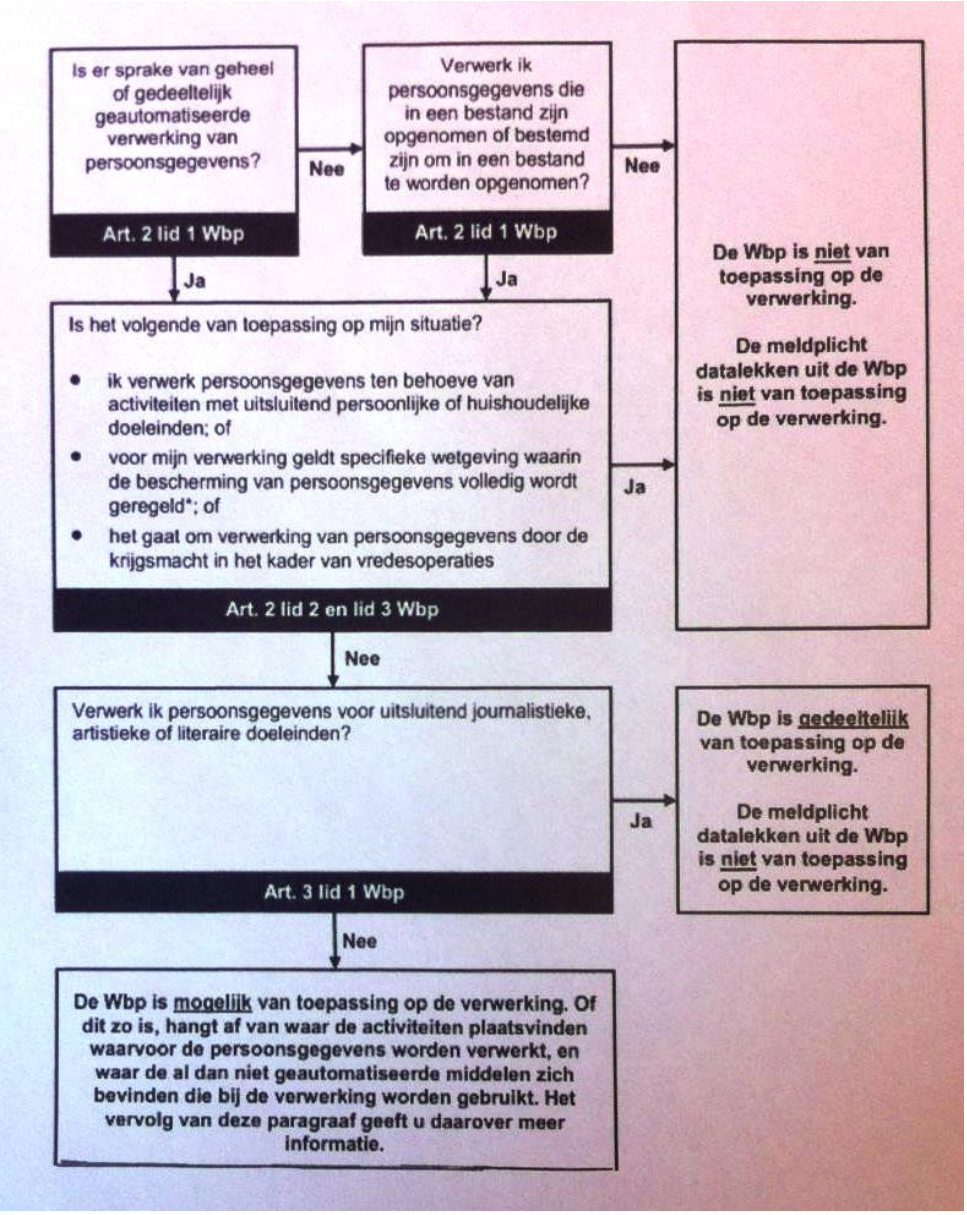


Aandachtspunten:

- Als u een aanbieder van een openbare elektronische communicatiedienst bent, dan heeft u te maken met twee meldplichten voor datalekken: de meldplicht in de Telecommunicatiewet (TW) en de meldplicht in de Wbp. Valt een datalek (gedeeltelijk) onder de meldplicht datalekken uit de TW? Ook dan moet u het datalek melden aan de Autoriteit Persoonsgegevens en mogelijk aan de betrokkene. In de WBP zijn voorzieningen opgenomen om dubbele meldingen te voorkomen.
- Deze beleidsregels treden in werking met ingang van 1 januari 2016, zijnde de datum van inwerkingtreding van de meldplicht datalekken. In de loop van 2017, of wanneer het aantal ontvangen meldingen daar aanleiding toe geeft, zullen deze beleidsregels worden geëvalueerd en waar nodig aangepast. Er zal dan opnieuw een consultatie plaatsvinden.
- Het toepassen van cryptografische bewerkingen zoals encryptie of *hashing* op identificerende gegevens leidt tot pseudonimisering (het vervangen van een identificerend gegeven door een ander identificerend gegeven) maar niet tot anonimisering.

Stroomschema's





Het schema 'Waar' (locatie) hebben we in dit document niet opgenomen omdat alle kerkelijke activiteiten van gemeenten zich in Nederland bevinden. Wanneer een gemeente toch voor buitenlandse projecten gegevens in of uit het buitenland verwerkt moet hier opnieuw naar worden gekeken. Denk hierbij aan adoptieprojecten en zending. Mogelijk heeft de gemeente dan te maken met andere wetgeving.

Derden in het spel

Bewerkers

Als u persoonsgegevens laat verwerken door een bewerker, dan moet u ervoor zorgen dat deze voldoende waarborgen biedt ten aanzien van de naleving van de meldplicht voor datalekken. U moet toezien op de naleving (artikel 14, eerste lid, Wbp).

U zorgt ervoor dat de bewerker de maatregelen treft die nodig zijn zodat u aan de meldplicht voor datalekken kunt voldoen (artikel 14, derde lid, sub c, Wbp).

In veel gevallen is de bewerker de eerste die kennis krijgt van een opgetreden datalek. Uw zorgplicht, als verantwoordelijke voor de verwerking, strekt zich expliciet uit over datalekken waarvan een bewerker kennis krijgt. Dat betekent dat u ervoor moet zorgen dat u, ook als u persoonsgegevens laat bewerken door een bewerker, in staat bent om uw wettelijke verplichtingen na te komen. In ieder geval moet u zorgen dat de bewerker u tijdig en adequaat informeert over de datalekken waarvan hij kennis krijgt.

Indien de concrete situatie zich daartoe leent, dan kunt u met de bewerker overeenkomen dat hij in het geval van een datalek de eerste melding aan de Autoriteit Persoonsgegevens doet. Voorwaarde is wel dat de bewerker, op basis van de afspraken die u met hem maakt, kan overzien in welke gevallen een melding aan de Autoriteit Persoonsgegevens noodzakelijk is. Als verantwoordelijke blijft u ook in dit geval eindverantwoordelijk voor de melding. Dit betekent dat u moet zorgen dat de bewerker u op de hoogte houdt als hij een datalek meldt aan de Autoriteit Persoonsgegevens.

Over de afspraken met bewerkers worden door de Autoriteit Persoonsgegevens voorstellen gedaan. Er is echter geen format. Wel zijn er sectoren die zelf een eigen regeling hebben ontworpen, zoals binnen de grafische industrie.

Belangrijk: een mondelinge overeenkomst is niet voldoende!

Voorbeelden waarbij de persoonsgegevens in gevaar komen:

- Een kwijtgeraakte USB-stick
- Een gestolen laptop
- Een inbraak door een hacker
- Een malware-besmetting
- Een calamiteit zoals brand in een datacenter

Bewerkersovereenkomst: verplichte onderdelen

Volgens de Wbp is het sluiten van een bewerkersovereenkomst verplicht tussen de verantwoordelijke voor persoonsgegevens en degene die de persoonsgegevens voor hem verwerkt. De bewerker mag alleen een externe partij inschakelen voor het verwerken van persoonsgegevens na schriftelijke toestemming van de verantwoordelijke.

De huidige verordening noemt onderwerpen die in de bewerkersoverkomst aanwezig moeten zijn. Dit zijn o.a.:

- Doel(en) van de gegevensverwerking
- De aard van de verwerkte persoonsgegevens
- Beveiliging van de gegevens
- Uitvoering van audits
- Bij beëindiging van de verwerking vernietigen of retourneren van de data aan de verantwoordelijke

Documentatieplicht: bijhouden register

De bewerker en de verantwoordelijke moeten een register bijhouden met daarin een beschrijving van de verwerking van persoonsgegevens. Zo'n register moet op elk moment een actueel en compleet inzicht geven, zoals: wat wordt opgeslagen, doel van de opslag, bewaartermijn, beveiligingsmaatregelen.
Voor organisaties met minder dan 250 medewerkers is het register niet verplicht, uitgezonderd bij structurele verwerking van persoonsgegevens of bij aanzienlijke risico's voor de betrokkenen.

Onderwerpen in een bewerkersovereenkomst

Over het algemeen zijn de onderstaande onderwerpen in de meeste bewerkersovereenkomsten terug te vinden.

- **Bewerking in overeenstemming met instructies verantwoordelijke**

De bewerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken, maar alleen om uitvoering te geven aan de instructies van de verantwoordelijke.

- **Geheimhouding**

In deze bepaling wordt aan de bewerker een geheimhoudingsplicht opgelegd, eventueel gecombineerd met een boetebeding. Overigens is opzettelijke niet-naleving van deze geheimhoudingsplicht strafbaar gesteld in het Wetboek van Strafrecht.

- **Beveiligingsmaatregelen**

De verantwoordelijke draagt zorg dat de bewerker passende technische en organisatorische maatregelen neemt om de persoonsgegevens te beveiligen tegen verlies e.d.

- **Inschakelen van derden en onderaannemers**

In de overeenkomst wordt vastgelegd of, en onder welke voorwaarden, de bewerker subbewerkers mag inschakelen.

- **Locatie van de data**

De verantwoordelijke moet weten in welke landen zijn data worden opgeslagen. Dit is mede van belang met het oog op de verplichtingen die gelden bij doorgifte van persoonsgegevens naar het buitenland.

- **Audits**

De verantwoordelijke moet kunnen controleren of de bewerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een audit (onderzoek) door de verantwoordelijke of door een onafhankelijke derde. In de bewerkersovereenkomst kunnen partijen hier nadere afspraken over maken.

- **Aansprakelijkheid**

De wet bepaalt dat de verantwoordelijke kan worden aangesproken als iemand schade lijdt doordat de Wet Bescherming Persoonsgegevens niet wordt nageleefd. Dit geldt zelfs als de schade het gevolg is van nalatigheid van de bewerker, die in dat geval ook zelfstandig aansprakelijk is. Het is verstandig in de bewerkersovereenkomst heldere afspraken te maken over deze verdeling.

Tenslotte

De naamgeving verandert overigens in 2018. Het begrip 'bewerker' wordt hernoemd in 'verwerker'. De 'bewerkersovereenkomst' wordt veranderd in 'verwerkersovereenkomst'.

Het bijhouden van logbestanden voor vaststellen wie toegang heeft tot data is relevant. Zie het al een digitaal logboek

Samengesteld team VKB
28 februari 2017

- 0 -