PROTOCOL DATALEKKEN van de Gereformeerde Gemeente van Alblasserdam

ALGEMEEN

Op grond van de AVG moet een datalek binnen 72 uur gemeld worden aan de Autoriteit Persoonsgegevens ('AP'). De melding kan gedaam worden via de website www.autoriteitpersoonsgegevens.nl.

Er hoeft geen melding te worden gedaan als het onwaarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van de betrokkenen. Daarnaast moet het datalek ook aan de betrokkene(n) gemeld worden indien het waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkene(n) met zich meebrengt.

Als er sprake is van een datalek wordt dat altijd (ook als er geen melding wordt gedaan bij de AP en/of bij de betrokkene(n)) in onze eigen administratie geregistreerd. Het model registratieformulier staat in bijlage 1.

Hieronder staat een stappenplan dat is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden.

Contactpersoon

Beveiligingsincidenten en/of datalekken kunnen gemeld worden aan de scriba. Zijn contactgegevens zijn de vinden op de website van onze gemeente.

Informeren

Degenen binnen de gemeente die persoonsgegevens verwerken weten wat een datalek is. Niet iedere inbreuk op de beveiliging is namelijk direct een datalek. Ook weten zij dat een datalek direct moet worden gemeld bij de scriba, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens indien dit is vereist. De scriba is bekend met het stappenplan datalekken.

Degenen binnen de gemeente die persoonsgegevens verwerken zijn verplicht om een (mogelijk) beveiligingsincident dat hij/zij ontdekt direct per e-mail of telefonisch aan de scriba te melden, ongeacht het tijdstip van de dag. Te denken valt aan:

- het laten liggen door van een laptop, tablet, smartphone of papieren dossier in de trein;
- het verliezen van een USB-stick, mobiele telefoon of bijvoorbeeld laptop;
- het verzenden van een e-mail aan meerdere ontvangers die elkaars emailadressen niet kennen (zonder gebruik te maken van de bcc-optie);
- fysieke diefstal van een laptop, tablet, smartphone of (onderdelen van een) papieren dossier;
- een hack;

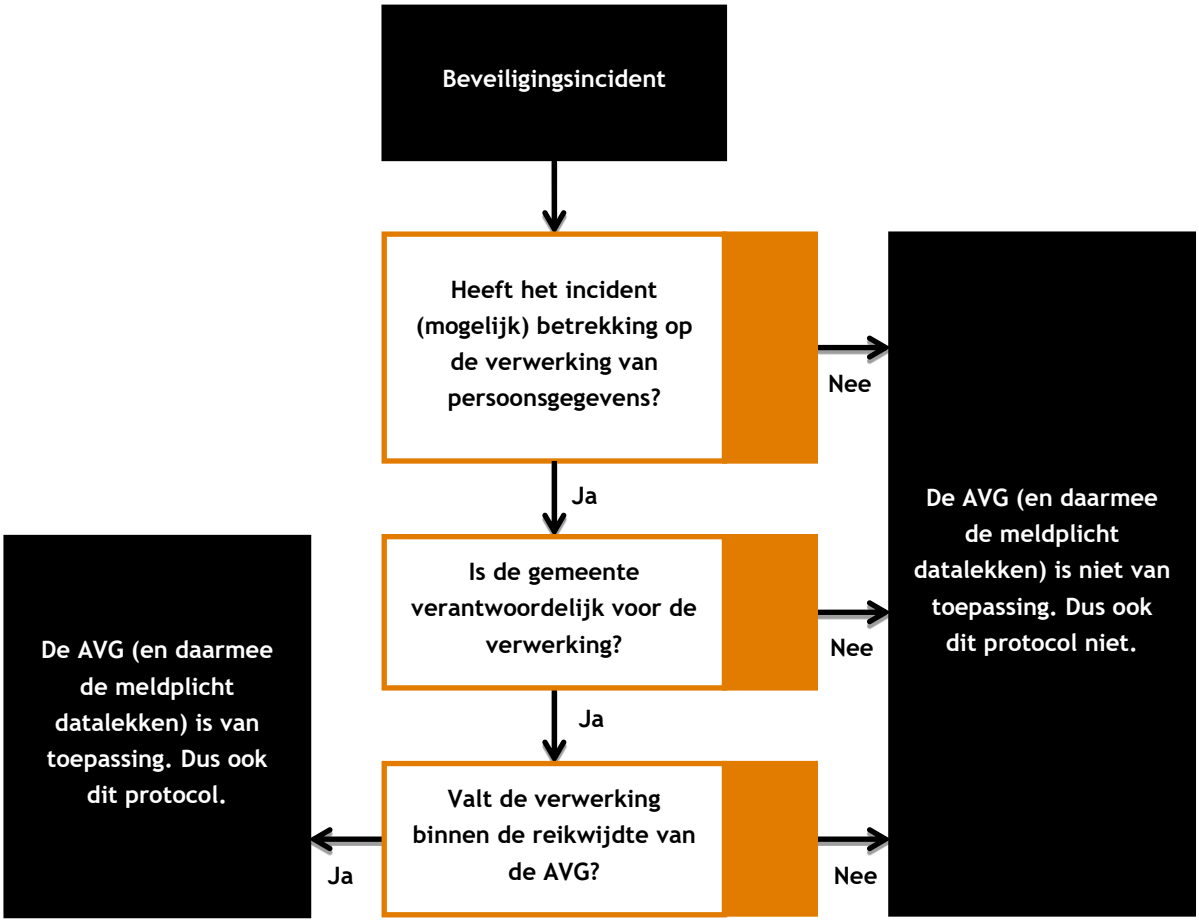
Indien zich een dergelijk- of soortgelijkend incident – voordoet, is er sprake van een beveiligingsincident en dient dit te worden gemeld aan de scriba. Als bijlage 2 bij dit protocol is een formulier toegevoegd om aan degenen binnen de gemeente die persoonsgegevens verwerken te verstrekken om hen bewust te maken van datalekken.

Uitvoeren van het stappenplan Datalekken

De scriba draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan Datalekken. De stappen worden gevolgd zodra melding is gemaakt van een datalek.

Stappenplan beoordeling mogelijk datalek:

Stap 1: is de AVG van toepassing?

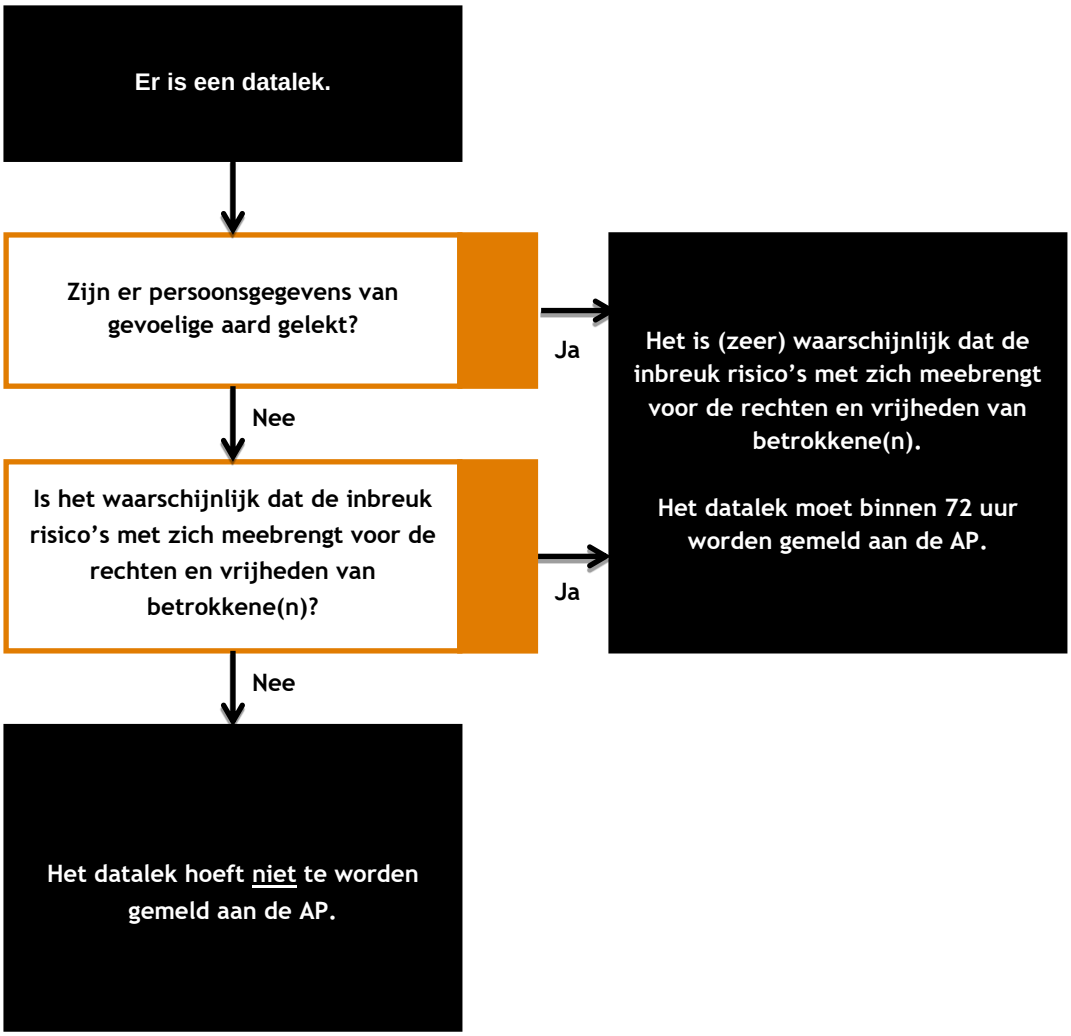


Stap 2: is er sprake van een datalek?

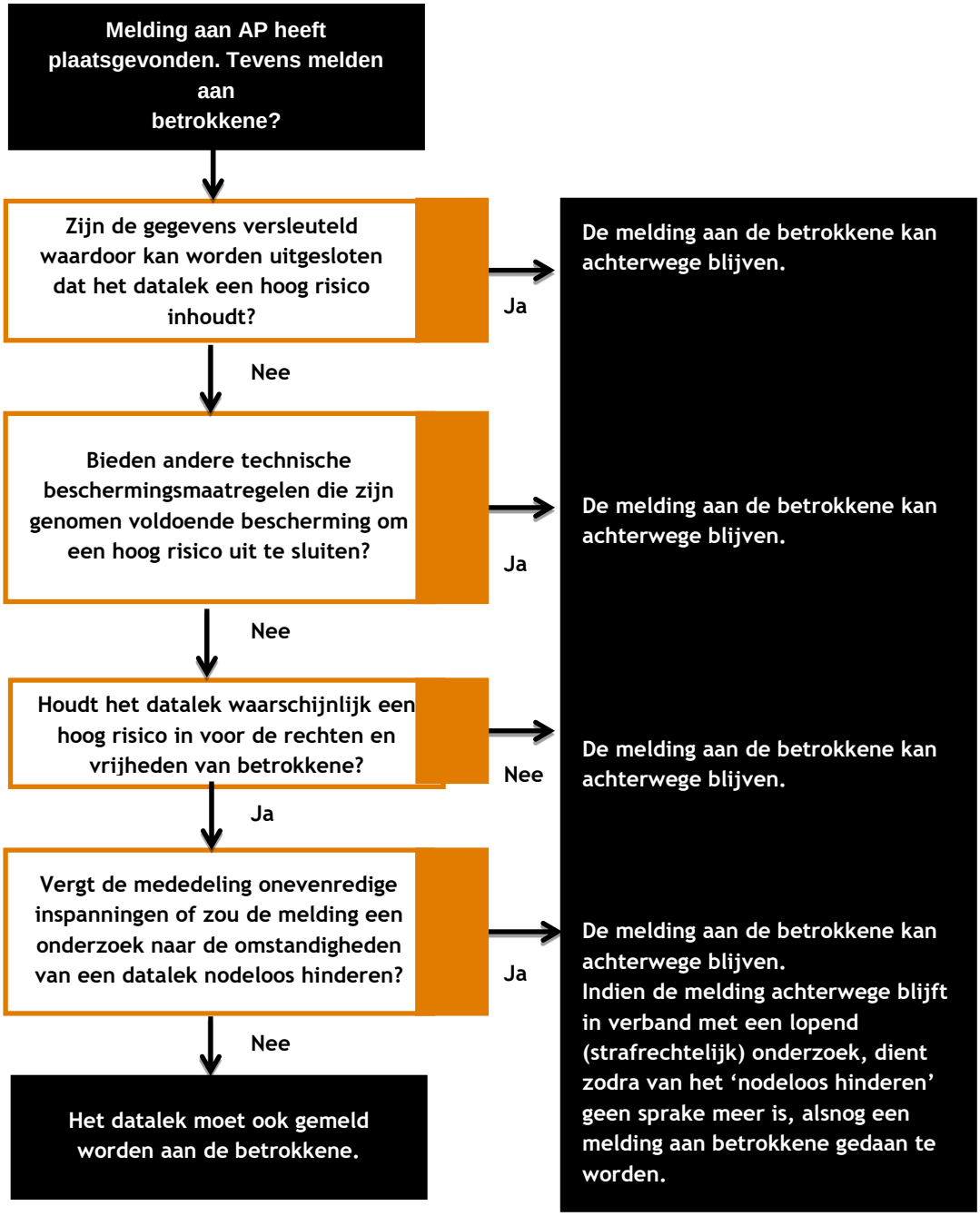
Beveiligingsincident: een inbreuk op de beveiliging die niet leidt tot vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens.

Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens.

Stap 3: moet het datalek worden gemeld aan de AP?



Stap 4: moet het datalek worden gemeld aan betrokkene?



Bijlage 1 - Model Intern Registratieformulier

Datum	**Beschrijving incident, soort gegevens en of er een (hoog) risico is voor de betrokkenen**	**Is het een datalek? (ja/nee)**	**Gemeld bij AP (ja/nee)**	**Gemeld bij betrokkenen (ja/nee)**	**Genomen maatregelen voor de toekomst**
bv. 3 maart 2019	*bv. Bij een brand in het kantoor zijn de personeelsdossiers van onze koster en organist verloren gegaan. Omdat er geen risico's zijn voor de rechten van de koster of de organist omdat de gegevens verloren zijn gegaan en niemand deze in kon zien, zijn er geen meldingen gedaan.*	*bv. ja*	*bv. nee*	*bv. nee*	*De gemeente heeft haar brandveiligheid nog een goed doorgenomen en heeft overspannings-stopcontacten gekocht.*

Bijlage 2 – Interne instructie melding datalekken

Sinds 1 januari 2016 dient een verwerkingsverantwoordelijke een zogenaamd datalek onverwijld te melden aan de Autoriteit Persoonsgegevens (AP) en mogelijk ook aan de betrokkene(n). Van een datalek dat moet worden gemeld is sprake indien er persoonsgegevens verloren gaan of onrechtmatig worden verwerkt en het waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

In het kader van deze wettelijke plicht heeft de gemeente een Protocol Datalekken opgesteld en geïmplementeerd. Onderdeel daarvan is ook deze instructie. Als de kerkenraad namelijk niet op de hoogte is van een mogelijk beveiligingsincident zal het Protocol Datalekken niet in werking (kunnen) treden. De kerkenraad is dan ook afhankelijk van de input die zij in dit verband krijgt van onder andere degenen binnen de gemeente die persoonsgegevens verwerken.

Meldingsplicht
Degenen binnen de gemeente die persoonsgegevens verwerken zijn verplicht een (mogelijk) beveiligingsincident dat hij/zij ontdekt direct per e-mail of telefonisch te melden aan de scriba ongeacht het tijdstip van de dag. Deze melding zal zo concreet mogelijk zijn.

Persoonsgegevens
Wat zijn persoonsgegevens? Dit zijn niet alleen gegevens zoals naam, adres, woonplaats of BSN-nummer. Deze gegevens worden aangeduid als direct identificerende gegevens. Daarnaast zijn er ook indirect identificerende gegevens. Dit zijn gegevens die iets zeggen over een natuurlijk persoon omdat zij gekoppeld kunnen worden aan een direct persoonsgegeven. Indien kan worden achterhaald om welke natuurlijke persoon het gaat, is er sprake van een persoonsgegeven. Het kan dus onder andere gaan om:

- naam;
- adres;
- telefoonnummer;
- e-mailadres;
- salarisgegevens;
- gegevens met betrekking tot ziekte;
- beoordelingsgesprekken;
- gegevens met betrekking tot gezondheid;
- betalingsachterstanden;
- gegevens over gezinssituatie;
- geloof;
- ras;
- etc.

Soorten beveiligingsincidenten
Er zijn verschillende soorten beveiligingsincidenten. Sommige beveiligingsincidenten zijn het gevolg van menselijke fouten, onoplettendheid of technisch falen. Deze beveiligingsincidenten worden niet bewust gecreëerd. Veel beveiligingsincidenten worden echter bewust gecreëerd.

Niet bewuste incidenten
Bij niet bewuste beveiligingsincidenten gaat het om incidenten die niet met opzet worden gecreëerd. Te denken valt aan:

- het laten liggen door van een laptop, tablet, smartphone of papieren dossier in de trein;
- het verliezen van een USB-stick, mobiele telefoon of bijvoorbeeld laptop;
- door haperende beveiliging (technische storing) zijn mogelijk persoonsgegevens ingezien door onbevoegden;
- de ruimte met daarin fysieke dossiers heeft per ongeluk niet op slot gezeten voor een bepaalde periode;
- iemand heeft per ongeluk onbeheerd zijn laptop laten staan met daarop een memo-sticker met zijn inlognaam en wachtwoord;
- het verzenden van e-mail met vertrouwelijke gegevens aan de verkeerde ontvanger;

- het verzenden van een e-mail aan meerdere ontvangers die elkaars emailadressen niet kennen (zonder gebruik te maken van de bcc-optie);
- het crashen van een harde schijf met daarop persoonsgegevens;
- brand in een serverruimte of archiefruimte van de gemeente;
- één van de hier voor genoemde situaties zich voordoet bij een verwerker van de gemeente (bijvoorbeeld: de drukker of de (salaris)administratie) voor zover het persoonsgegevens betreft van leden, personeel of andere betrokkenen van de gemeente.

Bewuste incidenten

Bij bewuste beveiligingsincidenten gaat het om incidenten die met opzet worden gecreëerd. Te denken valt aan:

- fysieke diefstal van een laptop, tablet, smartphone of (onderdelen van een) papieren dossier;
- het kopiëren, meenemen of bijvoorbeeld vernietigen van persoonsgegevens door een medewerker bijvoorbeeld uit onvrede over ontslag, als vriendendienst of als gevolg van chantage;
- phishing: het uitbuiten van menselijke kwetsbaarheden door hen onder valse voorwendselen persoonsgegevens te ontfutselen via mail of internet;
- hack: het uitbuiten van kwetsbaarheden in informatiesystemen en webservers;
- één van de hier voor genoemde situaties zich voordoet bij een verwerker van de gemeente voor zover het persoonsgegevens betreft van leden, personeel of andere betrokkenen van de gemeente.

Indien zich een dergelijk onbewust of bewust gecreëerd incident – of soortgelijkend incident – voordoet, is er sprake van een beveiligingsincident en dient de medewerker dit te melden aan de scriba.