Protocol datalek melden

Juni 2018

Inhoud

1. Inleiding

Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Deze meldplicht houdt in dat organisaties onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra een ernstig datalek wordt geconstateerd. Tevens dient men, in een aantal gevallen, het datalek ook te melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) formeel van kracht die de Wet bescherming persoonsgegevens heeft vervangen. Onder de AVG geldt tevens de meldplicht Datalekken.

1.1 Doel en reikwijdte

De AVG bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens ('AP'), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.
Aan de beantwoording van de vraag of er sprake is van een datalek moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn, dan is de melding meestal noodzakelijk.
Dit protocol datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden. Het protocol voorziet in een stappenplan ten aanzien van een beveiligingsincident en de afwegingen over de meldplicht Datalekken. Tevens is er een stroomschema bijgevoegd (zie bijlage).

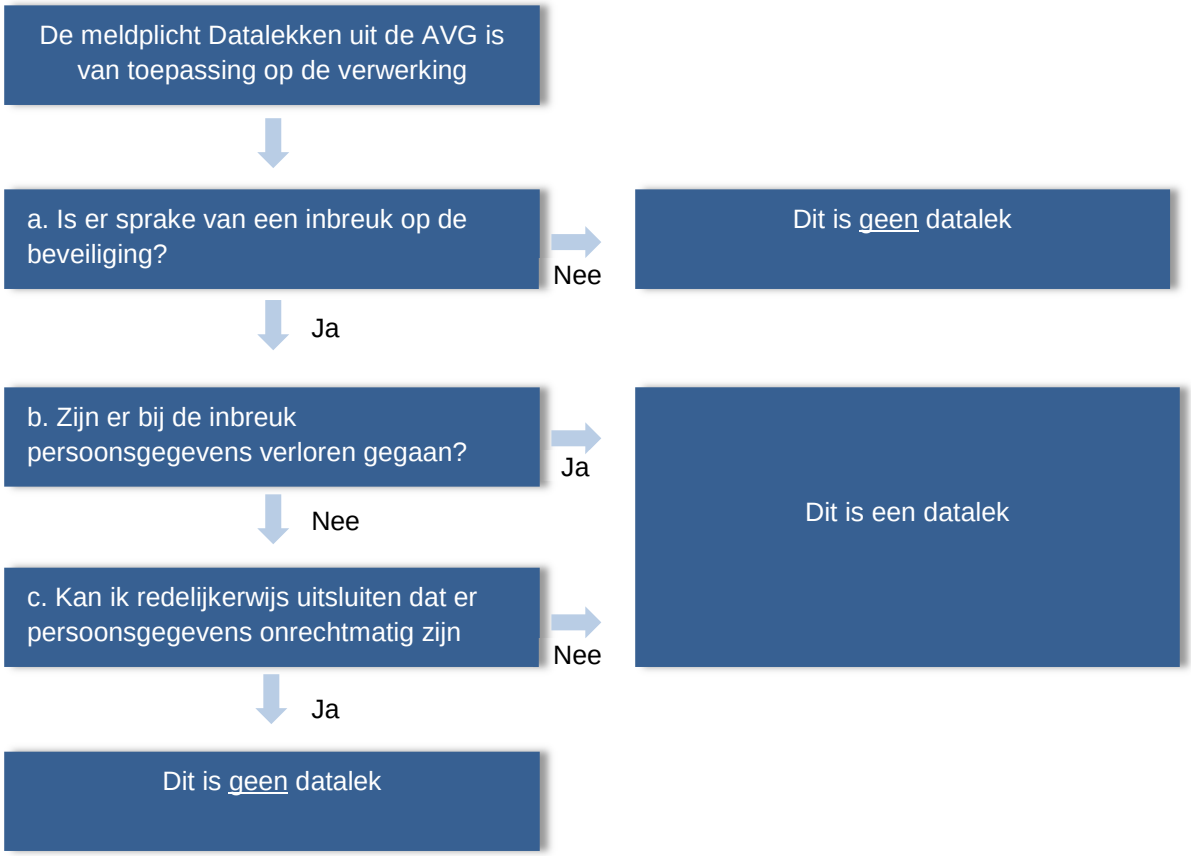
2. Wat is een datalek?

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.
Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.
Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- kwijtraken van een USB -stick
- diefstal van een laptop
- inbraak door een hacker
- persoonsgegevens per ongeluk gepubliceerd
- hacking, mailware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum

3. Stappenplan constatering (en melding) datalek

3.1 Zijn bij het beveiligingsincident gegevens verloren gegaan?



Toelichting:

a. Is er sprake van een inbreuk op de beveiliging? Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan en eventueel getroffen preventieve maatregelen waren niet toereikend om dit te voorkomen.

- **Voorbeelden**: een kwijtgeraakte USB-stick; een gestolen laptop; een inbraak door een hacker; een calamiteit zoals een brand in een datacentrum etc.
- **Kenmerken**: het beveiligingsincident heeft daadwerkelijk gevolgen voor de persoonsgegevens die worden verwerkt. Er zijn persoonsgegevens verloren gegaan of er kan niet redelijkerwijs uitgesloten worden dat er persoonsgegevens onrechtmatig zijn verwerkt. De repressieve maatregelen en de herstelmaatregelen die eventueel zijn getroffen waren niet voldoende om de gevolgen geheel weg te nemen.

b. Zijn bij de inbreuk persoonsgegevens verloren gegaan? Er is sprake van een datalek als de persoonsgegevens verloren zijn gegaan als gevolg van een calamiteit en er geen actuele reservekopie beschikbaar is.

c. Kan redelijkerwijs worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt?

Als redelijkerwijs niet uitgesloten kan worden dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet de inbreuk beschouwd worden als een datalek.

3.2 Melden aan de Autoriteit Persoonsgegevens

Er is sprake van een geclausuleerde meldplicht voor datalekken: een inbreuk hoeft alleen gemeld te worden als die waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkene (artikel 33 lid 1 AVG).

De gemeente bepaalt of een datalek dat is ontdekt binnen de reikwijdte van de meldplicht Datalekken aan de Autoriteit Persoonsgegevens valt. Deze afweging kan middels onderstaande vragen ondersteund worden:

Toelichting:

a. Zijn er persoonsgegevens van gevoelige aard gelekt?

Hierbij moet gekeken worden naar de aard van de getroffen gegevens. Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn?

Tot deze categorie van persoonsgegevens moet in ieder geval worden gerekend:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG: bijvoorbeeld over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid.
- Gegevens over de financiële situatie van betrokkene: bijvoorbeeld gegevens over schulden, salaris- en betalingsgegevens.

- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene: bijvoorbeeld gegevens over een gokverslaving, prestaties op school of werk of gegevens over een strafrechtelijke veroordeling of strafbare feiten.
- Gebruikersnamen, wachtwoorden en andere inloggegevens.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude: bijvoorbeeld kopieën van identiteitsbewijzen en Burgerservicenummer (BSN).

b. Leiden aard en omvang van de inbreuk waarschijnlijk tot een risico voor de rechten en vrijheden van betrokkene?

De aard en omvang van de getroffen verwerking moet mede bepalend zijn voor de beantwoording van de vraag of er bij een datalek waarschijnlijk sprake is van een risico voor de rechten en vrijheden van betrokkene. Beveiligingslekken in de omvangrijke verwerking van persoonsgegevens waarover de gemeente beschikt kunnen ook zeer grote gevolgen hebben voor betrokkenen.

Voorbeelden:

Enkele voorbeelden van datalekken welke moeten worden gemeld aan de Autoriteit Persoonsgegevens:

- Een overheidsdatabase met gevoelige persoonsgegevens wordt gehackt waardoor onbevoegden toegang hebben gekregen tot deze gegevens;
- Een medewerker verliest een USB of laptop met onversleutelde gegevens van burgers;
- Door een beveiligingslek blijkt dat persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen) van werknemers door onbevoegden zijn ingezien;
- Enkele personeelsleden maken gebruik van het wachtwoord van een ander persoon om toegang te krijgen tot persoonsgegevens. Er is op onrechtmatig wijze toegang verkregen tot persoonsgegevens. Bovendien is er sprake van een schending van interne voorschriften. Disciplinaire maatregelen liggen voorts voor de hand.

Enkele voorbeelden van gebeurtenissen die niet onder de meldplicht vallen:

- Een brief met daarin persoonsgegevens wordt naar een fout adres gestuurd, maar wordt ongeopend retour gezonden;
- Iemand laat een koffer met daarin persoonsgegevens achter in de trein, maar dit is voorzien van een deugdelijk slot en komt vervolgens ongeopend retour bij de eigenaar.

3.3 Wanneer en hoe dient het datalek gemeld te worden aan de Autoriteit Persoonsgegevens?

Het datalek moet zonder onredelijke vertraging gemeld worden aan de Autoriteit Persoonsgegevens (artikel 33 lid 1 AVG). Het zonder onredelijke vertraging melden houdt in dat, na het ontdekken van een mogelijk datalek, enige tijd genomen mag worden voor nader onderzoek teneinde een onnodige melding te voorkomen.

De termijn voor het melden van het datalek begint te lopen op het moment dat de gemeente zelf, of een verwerker die de gemeente heeft ingeschakeld, op de hoogte raakt van een incident dat mogelijk onder de meldplicht Datalekken valt.
Zonder onnodige vertraging, en zo mogelijk binnen **72 uur** na de ontdekking, dient melding te worden gedaan bij de Autoriteit Persoonsgegevens, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht Datalekken valt (artikel 33 lid 1 AVG). Indien het incident later dan 72 uur na ontdekking aan de toezichthouder wordt gemeld, dan kan desgevraagd gemotiveerd worden waarom de melding later is gedaan. Het is mogelijk dat na 72 uur na de ontdekking van het incident nog niet volledig inzichtelijk is wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval wordt de melding gedaan op basis van de gegevens waarover op dat moment wordt beschikt. Eventueel kan de melding naderhand nog aangevuld of ingetrokken worden.
Om datalekken tijdig te kunnen melden zullen ook goede afspraken gemaakt moeten worden met de verwerkers, zodat ook tijdig en adequaat informatie verstrekken over alle relevante incidenten.
De Autoriteit Persoonsgegevens heeft een webformulier beschikbaar gesteld waarmee datalekken kunnen worden gemeld. Vervolgens verstuurt de Autoriteit Persoonsgegevens per omgaande een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie zal contact worden opgenomen om de herkomst van de melding te verifiëren.

3.4 Dient het datalek gemeld te worden aan de betrokkene?

Volgens de AVG dient het datalek, naast de melding aan de Autoriteit Persoonsgegeven, eveneens aan de betrokkene te worden gemeld indien het datalek een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene (artikel 34 lid 1 AVG).
Het is aan de gemeente om te bepalen of een datalek dient te worden gemeld aan de betrokkene. Deze afweging kan middels onderstaande vragen ondersteund worden:

Toelichting:
a. Zijn passende technische en organisatorische beschermingsmaatregelen genomen en zijn deze toegepast op de persoonsgegevens waarop het datalek betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling ?
Indien passende technische en organisatorische beschermingsmaatregelen zijn genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan betrokkene achterwege blijven.

1. Zijn persoonsgegevens blootgesteld aan vernietiging of aantasting? Een datalek waarbij adequaat versleutelde persoonsgegevens niet alleen zijn blootgesteld aan onbevoegde kennisname, maar ook aan verlies of aan andere vormen van onrechtmatige verwerking, kan een hoog risico vormen voor de rechten en vrijheden van betrokkene en moet daarom mogelijk aan hem/haar worden gemeld.

2. Waren de persoonsgegevens versleuteld op het moment dat de inbreuk plaatsvond? Een datalek waarbij (ook) niet versleutelde persoonsgegevens zijn gelekt, kan een hoog risico vormen voor de rechten en vrijheden van betrokkene en moet daarom mogelijk aan hem of haar worden gemeld.
3. Is de versleuteling adequaat? Bij gebruik van cryptografische bewerkingen dient periodiek beoordeeld te worden of deze nog voldoende bescherming bieden.
4. Is het restrisico acceptabel? Per concreet geval zal beoordeeld moeten worden of de geboden bescherming voldoende is om de kennisgeving aan betrokkene achterwege te kunnen laten. Hierbij moet ook meegewogen worden welke gevolgen het voor de persoonlijke levenssfeer van de betrokkene kan hebben als een aanvaller er nu of in de toekomst alsnog in slaagt om kennis te nemen van de getroffen persoonsgegevens.

b. Zal het datalek waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkene?

Het datalek moet aan de betrokkene worden gemeld indien dit waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van hun persoonsgegevens namelijk in hun belangen worden geschaad. De schade kan van materiële of immateriële aard zijn. Onder immateriële schade kan worden verstaan: aantasting in eer en goede naam of identiteitsfraude.
Indien er persoonsgegevens van gevoelige aard zijn gelekt, dan moet ervan uitgegaan worden dat het datalek niet alleen gemeld moet worden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene. Door deze kennisgeving is de betrokkene alert op de mogelijke gevolgen van het datalek en kan hij/zij zich – voor zover dat mogelijk is – daartegen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen.
Indien de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen, kan worden afgezien van melding aan de betrokkene (artikel 34 lid 3 sub b AVG).

c. Zou de mededeling onevenredige inspanningen vergen?

De melding aan betrokkene mag achterwege blijven als dat onevenredige inspanningen zou vergen. Hierbij geldt wel dat in plaats daarvan een openbare mededeling of een soortgelijke maatregel dient plaats te vinden waarbij betrokkenen even doeltreffend worden geïnformeerd. (artikel 34 lid 3 sub c AVG).

3.5 Wanneer moet het datalek gemeld worden aan de betrokkene?

Indien is gebleken dat het datalek aan betrokkene gemeld dient te worden, dient dit onverwijld te geschieden (artikel 34 lid 1 AVG). Dit houdt in dat, na het ontdekken van het datalek, nog enige tijd genomen mag worden voor nader onderzoek. Dit zorgt ervoor dat de betrokkene op een behoorlijke en zorgvuldige manier geïnformeerd kan worden. Hierbij moet wel rekening worden gehouden met het

feit dat de betrokkene mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene wordt geïnformeerd, hoe eerder deze in actie kan komen. In de melding aan de Autoriteit Persoonsgegevens moet aangeven worden of het datalek al aan de betrokkene is gemeld en, wanneer dit niet het geval is, wanneer dit alsnog gedaan zal worden. De termijn die in de melding aan de Autoriteit Persoonsgegevens wordt aangegeven, moet ook worden nagekomen.

3.6 Hoe dient het datalek gemeld te worden aan de betrokkene?

Bij de kennisgeving aan de betrokkene dient in ieder geval vermeld te worden:

- Aard van de inbreuk;
- Instanties waar de betrokkene meer informatie over de inbreuk kan krijgen;
- Eventueel te treffen maatregelen die de betrokkene wordt aanbevolen om negatieve gevolgen van de inbreuk te beperken.

Bij het beschrijven van de aard van de inbreuk kan doorgaans volstaan worden met een algemene omschrijving. Voorts wordt hierbij de contactgegevens opgenomen zodat de betrokkene terecht kan indien hij/zij vragen heeft over het datalek. Verder kan aangegeven worden wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken.
Het belangrijkste is dat zoveel mogelijk betrokkenen bereikt worden met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zoveel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaalgesproken niet bereikt.

3.7 Wie is verantwoordelijk voor het melden aan de betrokkene?

De Functionaris Gegevensbescherming (FG) adviseert het college van burgemeester en wethouders over het al dan niet melden van het datalek aan de betrokkene. Alleen bij zwaarwegende redenen kan van het advies van de FG worden afgeweken. Indien het college van burgemeester en wethouders besluit om het datalek te melden aan betrokkene, is de leidinggevende van de betreffende afdeling waartoe de discipline behoort waarmee het datalek verband houdt, verantwoordelijk voor het verder afhandelen van de melding aan de betrokkene.

4. Begripsbepalingen

In dit protocol wordt verstaan onder:

a. AVG: Algemene verordening gegevensbescherming

b. Persoonsgegeven: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatie-gegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 sub 1 AVG).

c. Verwerkingsverantwoordelijke: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 sub 7 AVG). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking. De bevoegdheden kunnen soms in verschillende handen liggen, er is dan sprake van gezamenlijke verantwoordelijkheid.

d. Verwerker: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4 sub 8 AVG). Verwerkers zijn ketenpartners of derden zoals IT-leveranciers die zorg dragen voor het onderhoud en beheer van systemen en/of applicaties en/of gegevensbestanden waar persoonsgegevens onderdeel van uit maken of bij betrokken worden.

e. Betrokkene: Een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG).

f. Derde: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken (artikel 4 sub 10 AVG).

g. Ontvanger: Een natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt (artikel 4 sub 9 AVG).

h. Verwerking van persoonsgegevens: Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken verstrekken d.m.v. doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, aligneren of combineren, afschermen, wissen of vernietigen van gegevens (artikel 4 sub 2 AVG).

i. Verstrekking van persoonsgegevens: Het bekendmaken of ter beschikking stellen van persoonsgegevens.

j. Verzamelen van persoonsgegevens: Het verkrijgen van persoonsgegevens.

Bijlage: Stroomschema
Procedure melden datalek bij de Autoriteit Persoonsgegevens
Stroomschema weging meldplicht Datalekken