BEEKDAELEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Beekdaelen

Nr. 33067

12 februari

2019

Besluit van het college van burgemeester en wethouders van de gemeente Beekdaelen houdende regels omtrent AVG Protocol meldplicht datalekken

Samenvatting

Op 1 januari 2016 is de meldplicht datalekken als gevolg van een wijziging in de Wet Bescherming Persoonsgegevens (Wbp) in werking getreden. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens 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). Doordat de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 van toepassing is geworden, is de Wbp en daarmee de meldplicht komen te vervallen. In de AVG is echter een soortgelijke meldplicht voor datalekken opgenomen.

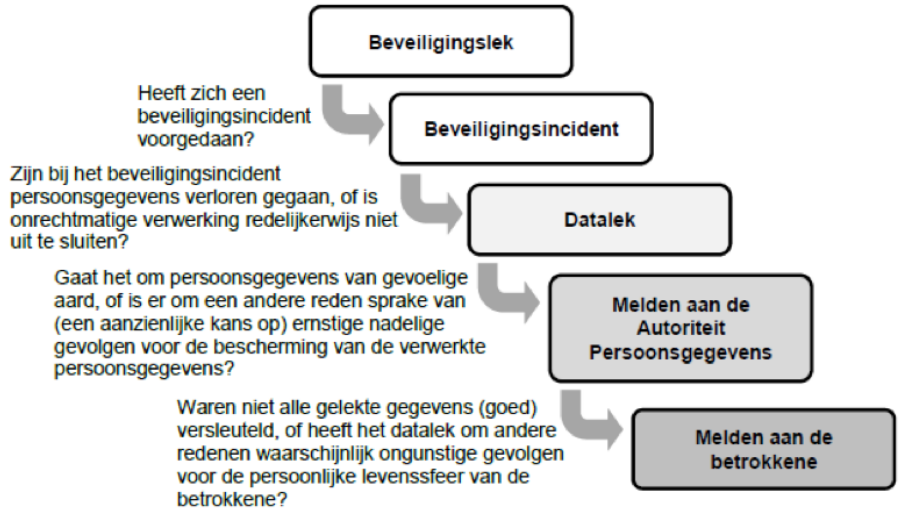
Kader

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de AVG. Hierin staat dat degene die persoonsgegevens verwerkt of laat verwerken, een passend gegevensbeschermingsbeleid moet uitvoeren dat past bij de aard, omvang, context en doel van de verwerking en de privacyrisico's voor betrokkenen (artikel 24 lid 2 AVG en artikel 32 AVG). Op grond van de AVG moet een inbreuk in verband met persoonsgegevens (hierna een "datalek" genoemd) worden gemeld aan de Autoriteit Persoonsgegevens als die waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokken personen (artikel 33 lid 1 AVG). Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene (artikel 34 lid 1 AVG).

Voorliggend protocol maakt deel uit van een groter geheel binnen de organisatie, namelijk het gegevensbeschermingsbeleid en het informatiebeveiligingsbeleid. Het gegevensbeschermingsbeleid dient ertoe bij te dragen dat er geen datalekken in de organisatie ontstaan. Voorts kan middels het informatiebeveiligheidsbeleid, alsmede de incidentmanagementprocedure, worden nagegaan of er sprake is van een datalek dan wel van een inbreuk op de beveiliging (hierna "beveiligingsincident" genoemd).

Afwegingen

Bij de beslissing of een gebeurtenis die zich heeft voorgedaan gemeld moet worden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, dient een aantal afwegingen gemaakt te worden. De Autoriteit Persoonsgegevens heeft – onder de Wbp – een afwegingskader opgesteld, dat stapsgewijs moet worden doorlopen. Het onderstaande schema geeft deze afwegingen weer.



Datalek

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet bijvoorbeeld gedacht worden aan het kwijtraken van een USBstick, diefstal van een laptop of een inbraak door een hacker.

Echter, niet ieder beveiligingsincident is ook een datalek. Volgens de AVG is er sprake van een datalek als een beveiligingsincident per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft dan geen melding gedaan te worden aan de Autoriteit Persoonsgegevens. Indien er sprake is van een beveiligingsincident dient, ongeacht of er sprake is van een datalek, de incidentmanagementprocedure te worden gevolgd.

Melden aan de Autoriteit Persoonsgegevens
Niet ieder datalek hoeft gemeld te worden aan de Autoriteit Persoonsgegevens. Volgens de wet dient slechts melding aan de Autoriteit Persoonsgegevens gedaan te worden, als het datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokken personen (artikel 33 lid 1 AVG).

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard kan gedacht worden aan:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG*
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en iemands genetische en biometrische gegevens met het oog op de unieke identificatie van een persoon.

- *Gegevens over de financiële of economische situatie van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris en betalingsgegevens.

- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen. Ook vallen hieronder gegevens over strafrechtelijke veroordelingen en strafbare feiten.

- *Gebruikersnamen, wachtwoorden en andere inloggegevens*
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude*
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat een datalek gemeld moet worden waarbij persoonsgegevens van slechts één persoon betrokken zijn.

Een melding moet gedaan worden zonder onnodige vertraging en zo mogelijk niet later dan **72 uur** na de ontdekking van het datalek (artikel 33 lid 1 AVG). Op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl) is voor dit doel een webformulier beschikbaar gesteld.
Via dit webformulier kan de melding indien nodig aangevuld of ingetrokken worden.

Melden aan de betrokkene
Als geconcludeerd wordt dat een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens, dan betekent dat niet automatisch dat dit datalek ook gemeld dient te worden aan de betrokkene. Hiervoor dient een aparte afweging gemaakt te worden.

De AVG geeft aan dat een melding gedaan moet worden aan de betrokkene als het datalek een hoog risico inhoudt voor diens rechten en vrijheden (artikel 34 lid 1 AVG).
Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij kan gedacht worden aan bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kan er in principe van uit gegaan worden dat het datalek niet alleen gemeld moet worden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.

De melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door bijvoorbeeld een gelekt wachtwoord te vervangen. De wet schrijft voor dat de melding onverwijld gedaan moet worden. Hierbij moet rekening worden gehouden met het feit dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet

nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover geïnformeerd wordt, hoe eerder hij/zij in actie kan komen.

Als passende technische beschermingsmaatregelen zijn genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, zoals versleuteling, of achteraf maatregelen zijn genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen, kan de melding aan de betrokkene achterwege blijven. Per geval dient bepaald te worden of de maatregelen die zijn getroffen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten. Ook indien de mededeling onevenredige inspanningen zou vergen, kan de melding aan de betrokkene achterwege worden gelaten. In dat laatste geval kan worden volstaan met een openbare mededeling of een soortgelijke maatregel (artikel 34 lid 3 AVG).

Register van datalekken
De AVG verplicht de gemeente als verwerkingsverantwoordelijke om alle datalekken bij te houden in een register, ongeacht of van die datalekken melding is gedaan bij de Autoriteit Persoonsgegevens en/of aan betrokkene. De Autoriteit Persoonsgegevens kan dat register opvragen en de gemeente, na beraad over de kans dat het datalek een hoog risico met zich meebrengt, verplichten alsnog melding te doen aan de betrokkene (artikel 34 lid 4 AVG).

Boete
Bij overtreding van de meldplicht datalekken uit de AVG kan de Autoriteit Persoonsgegevens een boete opleggen. Deze boete bedraagt maximaal 20 miljoen euro.
Indien de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan kan de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan eventuele oplegging van een bestuurlijke boete. Bij het opleggen van een boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Een omstandigheid van het geval kan bijvoorbeeld bestaan uit het feit dat de gegevens waarover het gaat niet door derden zijn ingezien.

Inleiding

Met ingang van 1 januari 2016 is een wijziging van de Wet bescherming persoonsgegevens (Wbp) in werking getreden die een meldplicht regelt voor datalekken. Doordat de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 van toepassing is geworden, is de Wbp en daarmee de meldplicht komen te vervallen. De AVG bevat echter een soortgelijke meldplicht voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens en in bepaalde situaties ook aan de betrokkene. De betrokkene is degene van wie persoonsgegevens zijn gelekt. Bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt moeten zelf een afweging maken of een concreet datalek, dat hen ter kennis komt, onder het bereik van de wettelijke meldplicht valt.

Dit protocol is gebaseerd op de beleidsregels van de Autoriteit Persoonsgegevens, die zijn opgesteld onder het regime van de Wbp. Deze beleidsregels hebben als uitgangspunt gediend voor het redigeren van dit protocol. Waar nodig dient in dit protocol voor (een betreffend artikel uit de) Wbp dan ook (het vergelijkbare artikel uit de) AVG te worden gelezen. Onderhavig protocol wordt regelmatig geëvalueerd en indien nodig worden herzien.

Verdere informatie over de beveiliging van persoonsgegevens en over de meldplicht datalekken is te vinden op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Leeswijzer
In het eerste hoofdstuk worden ingegaan op de uitleg van enkele belangrijke begrippen welke van betekenis zijn in voorliggend protocol. Voorts wordt in het tweede hoofdstuk, middels een schema en de beantwoording van een drietal vragen, nagegaan of de meldplicht datalekken al dan niet van toepassing is op de gemeente. In hoofdstuk drie wordt vervolgens ingegaan op het verwerken van persoonsgegevens door verwerkers. Hierbij wordt met name aandacht besteed aan het opstellen van afspraken met verwerkers in de vorm van verwerkersovereenkomsten. Het vierde hoofdstuk geeft voorts een stappenplan weer dat gevolgd kan worden om na te gaan of er sprake is van een datalek en of dit datalek al dan niet gemeld dient te worden aan de Autoriteit dan wel de betrokkene(n). In hoofdstuk vijf wordt kort weergegeven welke gegevens geïnventariseerd dienen te worden indien een datalek zich voordoet. In het zesde en tevens laatste hoofdstuk van dit protocol wordt ingegaan op het register van datalekken, alsmede eventuele handhavingsmogelijkheden welke ingezet kunnen worden door de Autoriteit Persoonsgegevens.

1. Definities

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, locatiegegevens, 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).

Bestand
Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel of functionele of geografische gronden is verspreid (artikel 4 sub 6 AVG).

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.

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). Verwerker zijn ketenpartners zoals Het Gegevenshuis of de salarisadministrateur die persoonsgegevens verwerken voor de gemeente of derden zoals ITleveranciers 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, zoals Parkstad IT voor de serversystemen.

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

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).

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).

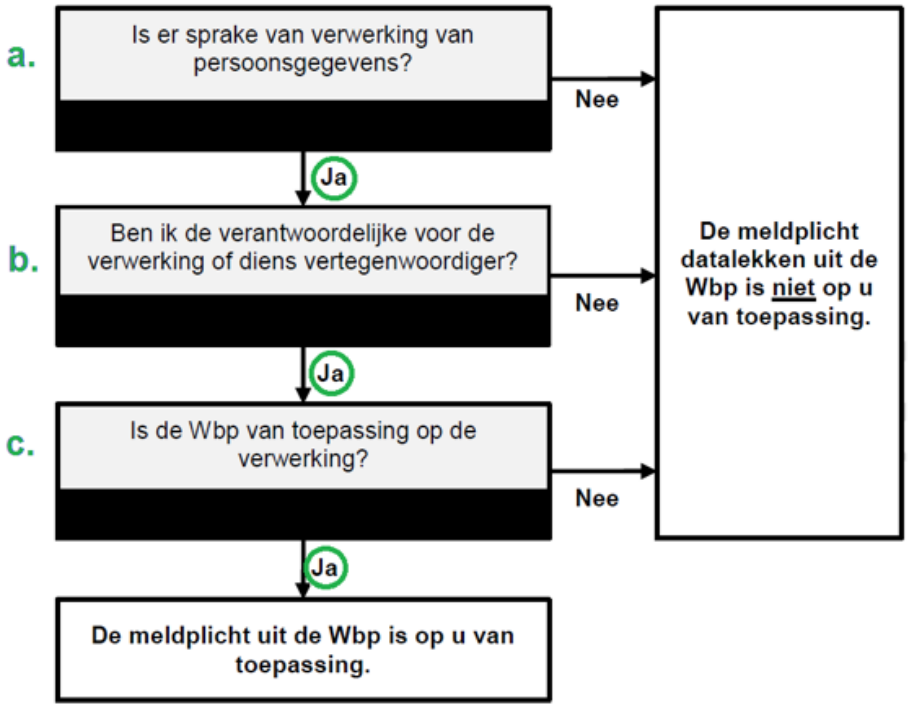
Verwerking van persoonsgegevens
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, 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).

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

Verzamelen van persoonsgegevens
Het verkrijgen van persoonsgegevens.

2. Is de meldplicht datalekken van toepassing?

Onderstaand schema geeft enkele vragen weer die beantwoord dienen te worden om vast te stellen of de meldplicht datalekken uit de AVG van toepassing is. Middels groene cirkels zijn de vragen vanuit het oogpunt van de gemeente beantwoord.



Toelichting:
a. Is er sprake van verwerking van persoonsgegevens?
Ja, er is binnen de gemeente sprake van verwerking van persoonsgegevens. Verwerking van persoonsgegevens betreft namelijk elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval 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).
b. Ben ik de verwerkingsverantwoordelijke voor de verwerking of diens vertegenwoordiger?
Voor veel verwerkingen is de gemeente verwerkingsverantwoordelijke voor de verwerking. De verwerkingvantwoordelijke is namelijk degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 sub 7 AVG). Een verwerkingsverantwoordelijke kan een vertegenwoordiger aanwijzen die namens hem de verplichtingen uit de AVG nakomt.
c. Is de AVG van toepassing op de verwerking?
De AVG is van toepassing op de verwerking wanneer deze geheel of gedeeltelijk geautomatiseerd is. Ook is de AVG van toepassing op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (artikel 2 lid 1 AVG). Bepaalde verwerkingen vallen buiten de reikwijdte van de AVG en op deze verwerkingen is de meldplicht datalekken niet van toepassing. Ten tweede is het van belang waar de activiteiten plaatsvinden waarvoor de persoonsgegevens worden verwerkt en waar de al dan niet geautomatiseerde middelen zich bevinden die bij de verwerking worden gebruikt. (zie artikel 2 lid 2 AVG)

3. Verwerking van persoonsgegevens door verwerker(s)

Verwerking van persoonsgegevens door verwerker(s) omvat onder andere:
- Persoonsgegevens die t.b.v. de gemeentelijke dienstverlening door ketenpartijen zoals Het Gegevenshuis of de salarisadministrateur worden verwerkt;
- ITleveranciers die een systeem of toepassing waarin persoonsgegevens worden verwerkt als cloudoplossing aanbieden;
- ITleveranciers die een systeem of toepassing beheren of onderhouden t.b.v. de gemeente.

Waarborgen
Bij verwerking door een verwerker dient de gemeente uitsluitend een beroep te doen op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische

maatregelen bieden zodat de verwerking aan de eisen van de AVG voldoet en de rechten van de betrokkenen zijn gewaarborgd (artikel 28 lid 1 AVG).

De gemeente is verplicht met verwerkers een verwerkersovereenkomst te sluiten, waarin afspraken met verwerkers worden gemaakt en vastgelegd ter borging van een zorgvuldige en rechtmatige gegevensverwerking (artikel 28 lid 3 AVG).

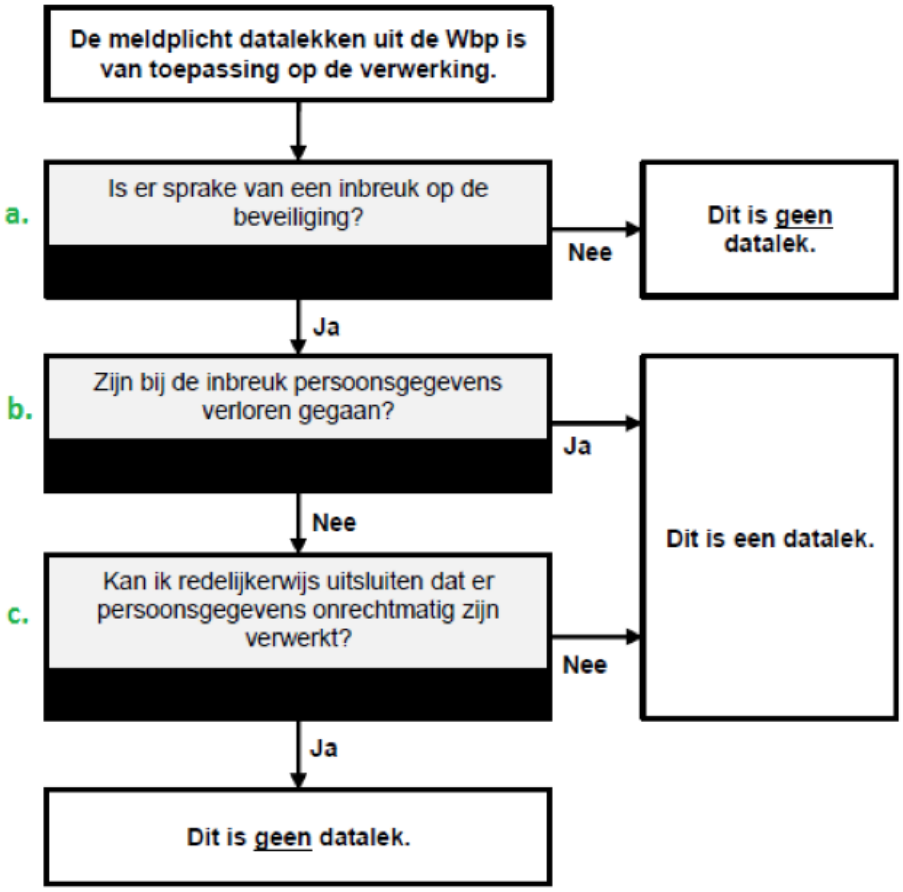
Waarover moeten afspraken gemaakt worden met de verwerker?
De AVG schrijft specifiek voor wat met een verwerker afgesproken dient te worden. In de overeenkomst dient het onderwerp, de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en plichten van de verwerkingsverantwoordelijke en de verwerker te worden omschreven. Meer specifiek dient de overeenkomst alle genoemde punten te bevatten uit artikel 28 lid 3 AVG, zoals het uitsluitend mogen verwerken op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, in acht nemen van vertrouwelijkheid, het nemen van passende beveiligingsmaatregelen, het verlenen van bijstand aan de verwerkingsverantwoordelijke bij de beantwoording van verzoeken van betrokkenen, het uitvoeren van audits en controles en in het kader van de meldplicht datalekken.

De verwerkingsverantwoordelijke moeten controleren of de afspraken in de verwerkersovereenkomst daadwerkelijk worden nageleefd.

Hoe moeten afspraken met de verwerker(s) worden gemaakt?
De afspraken tussen de gemeente en de verwerker(s) dienen schriftelijk vastgelegd te worden ingevolge artikel 28 lid 3 AVG in een verwerkersovereenkomst.

4. Stappenplan constatering (en melding) datalek

4.1 Nagaan of er sprake is van een datalek



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.

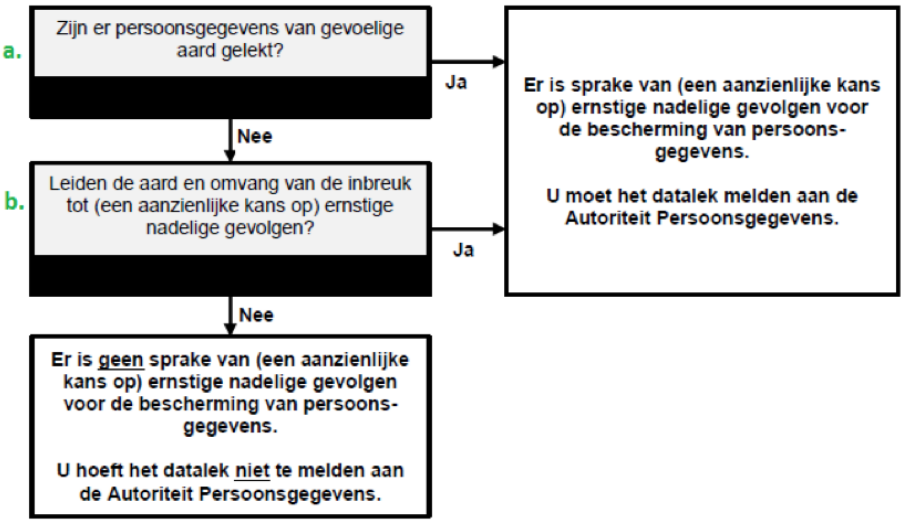
b. ***Zijn bij de inbreuk persoonsgegevens verloren gegaan?*** Er is sprake van een datalek als de persoonsgegevens verloren zijn gegaan als gevolg van een calamiteit en er geen actuele reservekopie beschikbaar is.

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.

4.2 Nagaan of er waarschijnlijk sprake is van een risico voor de rechten en vrijheden van betrokkene

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[1] :



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? Bij persoonsgegevens van gevoelige aard kunnen verlies of onrechtmatige verwerking o.a. leiden tot stigmatisering of uitsluiting van de betrokkene, tot financiële schade of (identiteits)fraude. Tot deze categorie van persoonsgegevens moet in ieder geval worden gerekend:

1) In het afwegingskader van de Autoriteit Persoonsgegevens wordt gesproken over "(een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens", waarbij melding moet worden gedaan aan de Autoriteit Persoonsgegevens. Aangezien het afwegingskader is opgesteld onder het regime van de Wbp en de terminologie uit de AVG daarvan afwijkt, dient in het afwegingskader de eerstgenoemde aanduiding te worden gelezen als de omschrijving uit artikel 33 lid 1 AVG "een waarschijnlijk risico voor de rechten en vrijheden van betrokkene".

- 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.

Behalve voor aard en omvang van de getroffen verwerking wordt ook aandacht gevraagd voor de positie van kwetsbare groepen (bijvoorbeeld mensen die te maken hebben met stalking of in een blijfvanmijnlijfhuis verblijven). Voor deze groepen kan verlies of onrechtmatige verwerking van persoonsgegevens extra risico's met zich meebrengen.

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.*

4.3. 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 gemotivverweerd 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.

4.4 Wie is verantwoordelijk voor de melding aan de Autoriteit Persoonsgegevens?

De medewerker die een (vermoedelijk) datalek ontdekt, meldt dit direct bij de Functionaris Gegevensbescherming (FG) of de Chief Information Security Officer (CISO) van de gemeente. Indien deze afwezig zijn meldt de medewerker dit bij zijn leidinggevende of een andere leidinggevende. De CISO of de leidinggevende neemt daarna direct contact op met de FG.

De FG gaat, eventueel in overleg met de CISO, na of sprake is van een datalek dat onder de meldplicht van de AVG valt. Indien dit het geval is, is de leidinggevende van de betreffende afdeling waartoe de discipline behoort waarmee het datalek verband houdt, verantwoordelijk voor het invullen en toezenden van het meldingsformulier aan de Autoriteit Persoonsgegevens binnen de termijn van 72 uur na ontdekking van het datalek. Bij diens afwezigheid is dat diens vervanger. De leidinggevende kan bij het invullen van het meldingsformulier zonodig overleg plegen met de Privacy Officer.

De leidinggevende of zijn vervanger zorgt voor een terugkoppeling van de melding aan de FG ten behoeve van diens register datalekken.

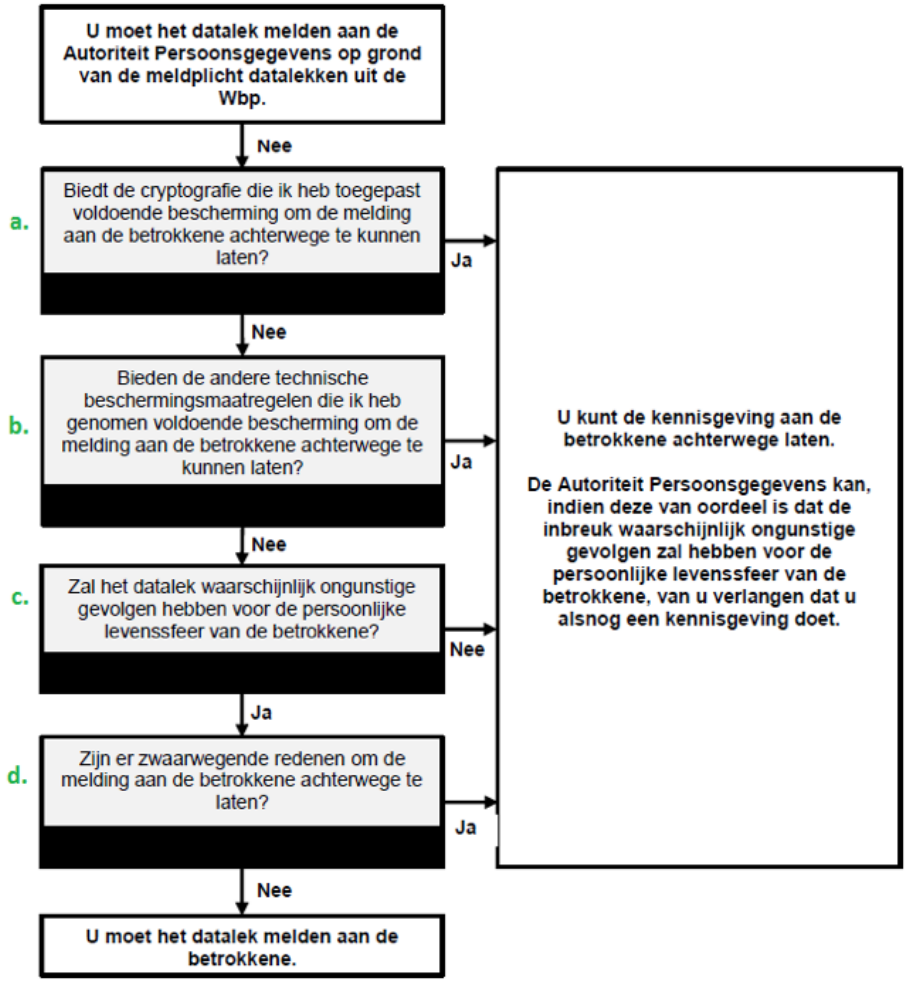
4.5 Dient het datalek gemeld te worden aan de betrokkene?

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 het orgaan dat verantwoordelijk is voor de betreffende gegevensverwerking (meestal is dit het college van burgemeester en wethouders, maar kan ook de burgemeester of de gemeenteraad zijn) om te bepalen of een datalek dient te worden gemeld aan de betrokkene. De FG adviseert het verantwoordelijk orgaan hierover. De afweging om het datalek wel of niet aan betrokkenen te melden kan middels onderstaande vragen ondersteund worden[2] :

4.5.1. Stappenplan melden aan betrokkenen ja/nee:

2) In het afwegingskader van de Autoriteit Persoonsgegevens, dat is opgesteld onder het regime van de Wbp, worden afwijkende termen gebruikt, dan die gelden volgens de AVG. De Autoriteit Persoonsgegevens spreekt over “biedt de cryptografie die is toegepast voldoende bescherming om melding aan de betrokkene achterwege te kunnen laten.” In het afwegingskader dient hiervoor te worden gelezen “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.” Tevens wordt in het afwegingskader gesproken over “waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkene.” Lees hier “waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen” Ook wordt gesproken over “bieden de andere technische beschermingsmaatregelen die zijn genomen voldoende bescherming om de melding aan betrokkene achterwege te laten.” Lees ook daarvoor “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.” Tenslotte: “zijn er zwaarwegende redenen om de melding achterwege te laten.” Lees daarvoor: “zou de mededeling onevenredige inspanningen vergen waardoor de melding achterwege moet blijven.” (Zie art. 34 AVG)



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 ? [3]

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.

Er zijn twee soorten cryptografische bewerkingen:

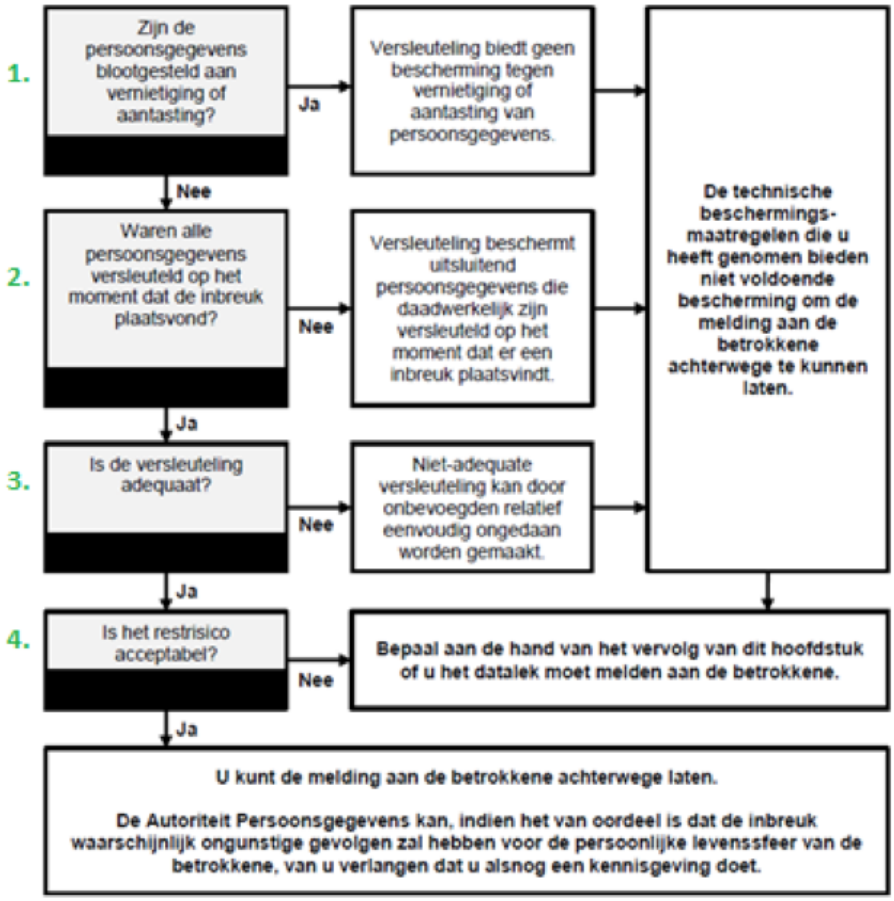
- Encryptie = versleuteling. Deze bewerking is omkeerbaar aangezien door gebruik van de juiste sleutel de oorspronkelijke informatie kan worden verkregen (decryptie)
- Hashing = het omzetten van gegevens in een unieke code. Hashing wordt onder meer gebruikt bij de opslag en verwerking van wachtwoorden.

Voorts vallen hieronder technische beschermingsmaatregelen als “remote wiping” en “pseudonimisering”. Middels “remote wiping” worden persoonsgegevens beschermd tegen onbevoegde kennisname. Bij deze methode wordt gegevens die op een apparaat staan op afstand gewist en daardoor ontoegankelijk voor onbevoegden. “Pseudonimisering” betekent dat technische maatregelen worden genomen om te voorkomen dat persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene. Het zorgt ervoor dat persoonsgegevens onbegrijpelijk worden gemaakt voor

3) In het afwegingskader van de Autoriteit Persoonsgegevens, dat is opgesteld onder het regime van de Wbp, worden afwijkende termen gebruikt, dan die gelden volgens de AVG. De Autoriteit Persoonsgegevens spreekt over “biedt de cryptografie die is toegepast voldoende bescherming om melding aan de betrokkene achterwege te kunnen laten.” In het afwegingskader dient voor deze term te worden gelezen “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.” (artikel 34 lid 3 sub a AVG).

onbevoegden en de kans dat een datalek een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen als gevolg daarvan wordt verlaagd.

Onderstaand wordt een aanvullend schema weergegeven ter beoordeling of de technische en organisatorische beschermingsmaatregelen die genomen zijn voldoende bescherming hebben geboden om melding aan de betrokkene achterwege te kunnen laten [4] :



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.

4) Zie hiervoor de tekst van de voetnoten nrs. 2 en 3.

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).

4.5.2 Wanneer moet het datalek gemeld worden aan de betrokkene?
Indien is besloten om het datalek aan betrokkene te melden, 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.

4.5.3 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.

4.5.4 Wie is verantwoordelijk voor het melden aan de betrokkene?
De FG adviseert het orgaan dat verantwoordelijk is voor de betreffende gegevensverwerking (meestal is dit het college van burgemeester en wethouders, maar kan ook de burgemeester of de gemeenteraad zijn) 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 verantwoordelijke orgaan besluit om het datalek te melden aan betrokkene, is de leidinggevende van de betreffende afdeling waartoe de discipline behoort waarmee het datalek verband houdt, of zijn vervanger, verantwoordelijk voor het verder afhandelen van de melding aan de betrokkene. De leidinggevende kan daarbij zonodig overleg plegen met de Privacy Officer.

De leidinggevende of zijn vervanger zorgt voor een terugkoppeling van de melding aan de FG ten behoeve van diens register datalekken.

BEEKDAELEN

5. Welke gegevens moeten worden vastgelegd?

De AVG bepaalt dat de gemeente een overzicht moet bijhouden van alle datalekken die hebben plaatsgevonden, ongeacht of deze datalekken zijn gemeld aan de Autoriteit Persoonsgegevens of aan betrokkenen. Per datalek bevat het overzicht in ieder geval feiten omtrent de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen (artikel 33 lid 5 AVG).

Daar de wet niet voorschrijft hoelang het overzicht bewaart moet worden, mag worden uitgegaan van een bewaartermijn van minimaal een jaar. Indien technische of organisatorische beschermingsmaatregelen voldoende bescherming hebben geboden om de melding aan de betrokkene achterwege te kunnen laten, als achteraf maatregelen zijn genomen om te zorgen dat er zich waarschijnlijk geen hoog risico meer zal voordoen voor de rechten en vrijheden van betrokkene, of als er andere redenen zijn geweest om de melding aan betrokkene achterwege te laten, dan dient het overzicht minimaal drie jaar te worden bewaard. Hierbij dient periodiek geëvalueerd te worden of het datalek alsnog aan de betrokkene gemeld moet worden.

Gegevens worden bewaard voor de volgende doeleinden:
- Lering trekken uit het datalek en de wijze waarop is gehandeld;
- Antwoord kunnen geven op vragen van betrokkenen en anderen;
- Alsnog melden van het datalek aan betrokkenen indien dit in eerste instantie achterwege is gelaten en de omstandigheden vereisen dat dit alsnog wordt gedaan.

Er dient rekening te worden gehouden met de mogelijkheid dat de Autoriteit, na beraad over de kans dat het datalek in verband met persoonsgegevens een hoog risico met zich meebrengt, de gemeente kan verplichten om het datalek alsnog te melden aan betrokkene. Ook dient de gemeente erop bedacht te zijn dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel of strafrechtelijk), en dat indien dit aan de orde is, bewijsmateriaal verzameld moet worden.

6. Wat doet de Autoriteit Persoonsgegevens met de melding?

Na het melden van een datalek stuurt de Autoriteit Persoonsgegevens per omgaande een ontvangstbevestiging. Als de melding de Autoriteit Persoonsgegevens aanleiding geeft tot nadere actie, dan zal deze daarover contact opnemen.

Het is de eigen verantwoordelijkheid om de oorzaak van het datalek op te sporen en om maatregelen te treffen om herhaling te voorkomen. Het is ook de eigen keuze om de betrokkene al dan niet te informeren.

De ontvangen datalekmeldingen stellen de Autoriteit Persoonsgegevens in staat om erop toe te zien dat betrokkenen adequaat worden geïnformeerd over datalekken die hen persoonlijk raken of waarvan zij last kunnen ondervinden. Als het datalek niet is gemeld aan de betrokkene en deze waarschijnlijk een hoog risico met zich meebrengt voor de rechten en vrijheden van betrokkene, kan de Autoriteit verlangen dat alsnog een kennisgeving wordt gestuurd (artikel 34 lid 4 AVG). Dit staat gelijk aan een bindende aanwijzing. Het niet nakomen kan voorts worden bestraft met een boete.

6.1 Lijst van ontvangen datalekmeldingen

De Autoriteit Persoonsgegevens stelt jaarlijks een verslag over haar activiteiten op met daarin mogelijk een lijst van de soorten gemelde datalekken en de soorten corrigerende maatregelen die zij daarop heeft genomen (artikel 59 AVG).

6.2 Handhaving

De Autoriteit houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en kan derhalve onderzoek doen naar de mogelijke overtredingen van de wet (artikel 58 AVG). Hiervoor kan de Autoriteit gebruik maken van informatie uit de ontvangen datalekmeldingen.

Bij overtreding van datgene dat bij of krachtens artikel 33 en 34 AVG wordt bepaald, heeft de Autoriteit Persoonsgegevens een breed scala van corrigerende maatregelen tot zijn beschikking (zie artikel 58 lid 2 AVG). Het opleggen van een boete is één daarvan. Als sprake is van een overtreding van de AVG die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, kan de toezichthouder direct een boete opleggen. Indien er geen sprake is van een overtreding van de AVG die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, zal waarschijnlijk een bindende aanwijzing

voorafgaan aan het opleggen van een boete. De Autoriteit kan de overtreder dan een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd. Bij het opleggen van een boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval.