Coöperatie Boer en Zorg b.a.

Procedure meldplicht datalekken

Inhoud

1. Aanleiding

Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Dit houdt in dat coöperatie Boer en Zorg verplicht is om (potentiële) datalekken te melden aan de toezichthouder, de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene van wie de gegevens zijn gelekt. Als blijkt dat niet of onvoldoende is voldaan aan deze meldplicht kan de toezichthouder een boete opleggen tot € 20 miljoen of 4% van de jaarlijkse wereldwijde omzet per overtreding.

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) formeel van kracht die de huidige Wet bescherming persoonsgegevens (Wbp) zal vervangen. Onder de AVG geldt tevens de meldplicht datalekken. Er zijn echter wel een aantal veranderingen ten opzichte van de Wbp, die tot een lichte wijziging in de huidige procedure leidt.

Volgens de AVG is er sprake van een datalek als zich een inbreuk voordoet op de beveiligingsmaatregelen, wat leidt tot het per ongeluk, opzettelijk of onrechtmatig vernietigen, verliezen, aanpassen, ongeautoriseerde openbaring van, of toegang tot, persoonsgegevens die overgedragen, bewaard of op een andere manier verwerkt zijn. Voorbeelden van een datalek zijn het verlies van een mobiel apparaat waarop gevoelige persoonsgegevens staan. Maar ook computer hacking, besmetting met ransomware, of het technische falen van apparatuur, stroomuitval, wateroverlast kunnen leiden tot een datalek.

Een datalek dient uiterlijk *binnen 72 uur* na ontdekking van het datalek te worden gemeld aan de toezichthouder. Indien dit later gebeurt, dan dient de melding voorzien te worden van uitleg omtrent de vertraging.

Niet ieder datalek-incident valt onder de meldplicht. Er is sprake van een zogeheten geclausuleerde meldplicht voor datalekken. Hiervoor is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Artikel 33(1) van de AVG stelt dat een datalek alleen gemeld dient te worden wanneer er een aanzienlijk risico is op schade aan de persoonlijke levenssfeer van een individu. Als bijvoorbeeld verloren of gesloten persoonsgegevens goed versleuteld zijn opgeslagen, dan is er geen aanzienlijke risico op schade aan de persoonlijke levenssfeer.

1.1. Doel en reikwijdte

Deze procedure beschrijft de wijze waarop binnen de organisatie van coöperatie Boer en Zorg wordt omgegaan met de meldplicht datalekken in de zin van de Algemene Verordening Gegevensbescherming (AVG). Het bevat afwegingskaders bij een vermoeden van een datalek en specificeert de nodige acties.

Binnen Boer en Zorg worden de volgende stappen in de procedure gehanteerd:

1) het signaleren, analyseren en registreren van incidenten waarbij er sprake is van een inbreuk op een beveiligingsmaatregel en persoonsgegevens betrokken zijn;
2) het inhoudelijk beoordelen en onderzoeken van het incident of er op grond van de AVG sprake is van een datalek dat gemeld moet worden;

3) het melden van het datalek aan de toezichthouder en betrokkenen namens het bestuur;
4) het nemen van maatregelen om het lek te dichten;
5) het documenteren van het datalek bij zowel interne als externe meldingen.

Hieronder volgt een nadere uitwerking van deze procedure.

2. Procedure Datalek

2.1. Melden incident bij FG

De meldplicht datalekken geldt voor de gehele organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van Boer en Zorg zijn, of met een informatiebeveiligingsincident, dient dit te melden bij de FG. Dit kan telefonisch (0317) 479 745 of via e-mail info@boerenzorg.nl

De medewerker wordt verzocht zijn/haar naam en contactgegevens in het formulier in te vullen met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en de volledigheid voor een eventuele melding aan de AP.
Indien de medewerker twijfelt of er sprake is van een incident of wat hij moet doen, kan hij de FG hiervoor benaderen.

2.1.1. Registratie

De medewerker FG registreert de incidentmelding in Afas.

De medewerker FG analyseert of er bij het incident persoonsgegevens betrokken zijn. Indien de melding telefonisch is gedaan, vraagt de medewerker dit na bij de melder.

2.2. Beoordelen of er sprake is van een datalek

Zo snel mogelijk na de melding van een incident beoordeelt de FG of er sprake is van een datalek dat valt onder de meldplicht van de AVG.

De FG beoordeelt het incident en besluit of er sprake is van een datalek dat gemeld moet worden aan de toezichthouder of de betrokkene.

De FG is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd naar de toezichthouder. Vanwege het gegeven dat een (zorg)organisatie binnen 72 uur behoort te melden aan de toezichthouder dient de melding door alle betrokken medewerkers *direct en met hoogste prioriteit* te worden opgepakt.

De FG houdt een register bij waarin alle datalekken die zich voordoen in de organisatie geregistreerd worden. Dit betekent dat ook wanneer een lek niet gemeld hoeft te worden, er een documentatieplicht geldt.

2.2.1. Beslisboom voor de melding aan toezichthouder

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat alleen een inbreuk hoeft te worden gemeld als deze leidt tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van betrokkenen. Hierbij spelen de volgende factoren een rol:

1) Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals medische/politiegegevens gegevens over ras of religie of financiële gegevens zijn gelekt.
2) Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.

Er moet in ieder geval gemeld worden als één van onderstaande vragen positief wordt beantwoord.

Zijn gegevens (definitief) verloren gegaan? Ja → melden
Zijn de gegevens bijzonder of zeer omvangrijk? Ja → melden
Zijn de gegevens in onbevoegde handen geraakt? Ja → melden
Aanzienlijk risico op schade aan persoonlijke levenssfeer? Ja → melden Nee op alle vragen →niet melden

Mogelijk is op het moment dat er gemeld moet worden nog geen volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval vindt de melding plaats op basis van de gegevens waarover Boer en Zorg op dat moment beschikt. Eventueel kan de melding naderhand nog worden aangevuld of zelfs worden introkken.

2.2.2. Melden aan betrokkene?

De betrokkene is degene over wie persoonsgegevens worden verwerkt en waarvan de gegevens onderwerp zijn van het datalek. Indien er sprake is van een datalek moet deze aan de betrokkene worden gemeld, als de inbreuk een hoog risico brengt op schade aan diens persoonlijke levenssfeer. Niet in alle gevallen hoeft een datalek aan de betrokkene te worden gemeld.

Voor de beoordeling of aan de betrokkene(n) gemeld moet worden, zijn de volgende vragen van belang.

Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten? Nee → melden betrokkene

Zijn de gegevens versleuteld of ontoegankelijk voor degene die geen recht op inzage heeft in deze gegevens? Nee → melden betrokkene

Artikel 34(3) van de AVG stelt drie voorwaarden waaronder geen melding aan betrokkenen vereist is. Dit geldt in de volgende situaties:

1. Er zijn technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens vooraf aan het lek. In het bijzonder maatregelen die ervoor zorgen dat de data niet toegankelijk is voor ongeautoriseerde personen. Bijvoorbeeld door encryptie of anonimiseren.
2. Direct na een datalek zijn er acties ondernomen om ervoor te zorgen dat er geen hoog risico meer is op schade aan de persoonlijke levenssfeer van betrokkenen.
3. Het zou van onevenredige moeite zijn om contact op te nemen met individuen, bijvoorbeeld wanneer de contactgegevens van betrokkenen verloren zijn. In dit geval zal er gekozen moeten worden voor een openbare communicatie uiting of een vergelijkbare maatregel.

Termijn van melden
Voor het melden van een datalek aan betrokkenen geldt dat dit ‘onverwijld’ moet gebeuren. Uitgangspunt is dat onnodige vertraging wordt voorkomen, zodat de betrokkene de nodige maatregelen kan treffen. Gelet hierop dient een datalek binnen 72 uur te worden gemeld aan de toezichthouder. De wijze waarop betrokkenen worden geïnformeerd, bepaalt Boer en Zorg zelf.

2.2.3. Melden aan andere partijen?

Indien sprake is van samenwerking met andere partijen (ketenverwerking of verwerkers) zal Boer en Zorg moeten beoordelen of een datalek-incident aan de externe partij gemeld moet worden. Dit is geen wettelijke verplichting, maar kan vanuit communicatie redenen raadzaam zijn.
Bij de uitwerking van de communicatiestrategie vindt afstemming plaats welke doelgroepen/ overige partijen worden geïnformeerd over het datalek en op welke wijze.

2.3. Melden aan de toezichthouder en betrokkene(n)

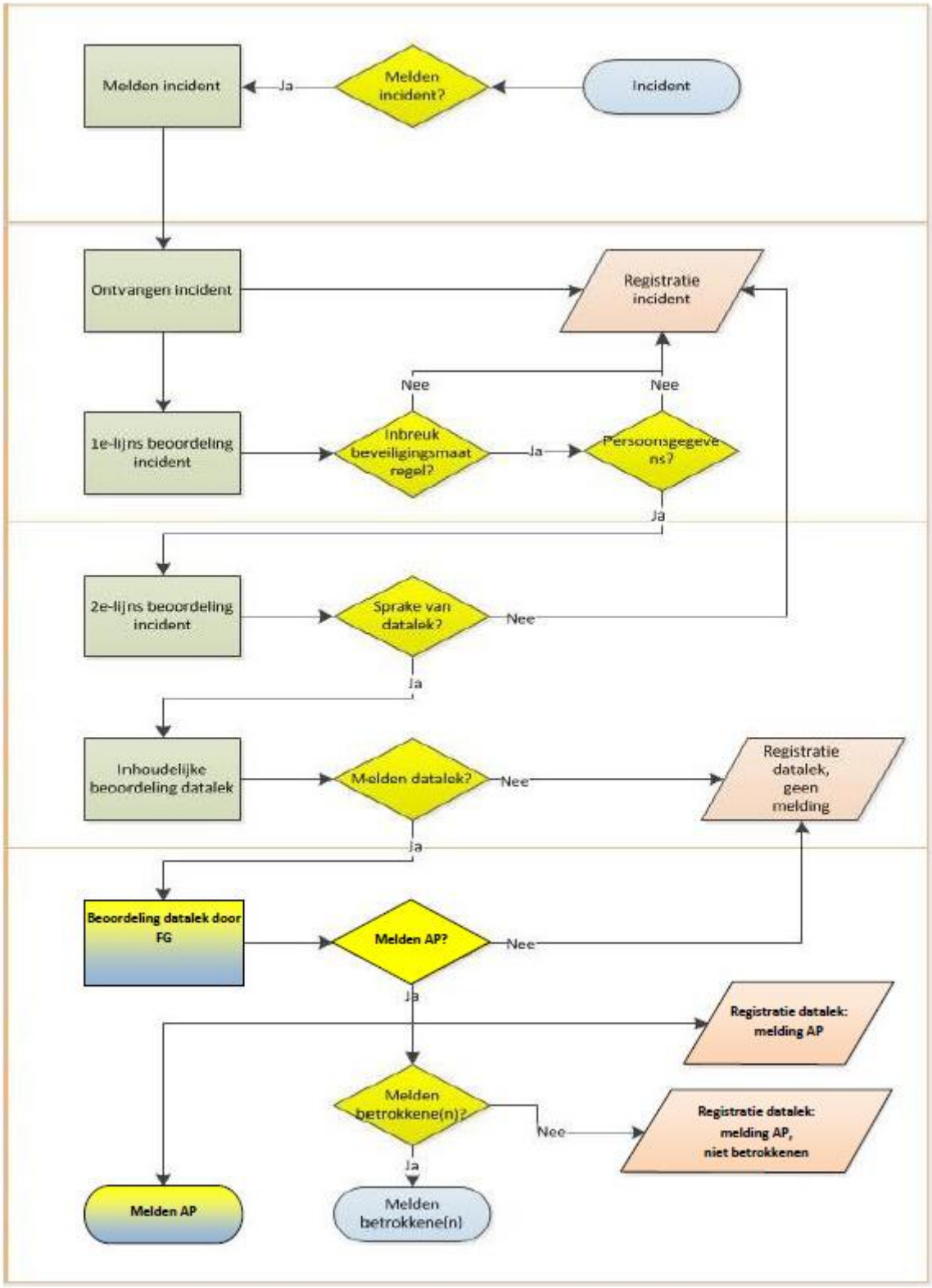
Het bestuur is eindverantwoordelijk voor het voldoen aan de meldplicht datalekken. Op grond van de mandaatregeling meldt de FG namens het bestuur/ de directeur bestuurder het datalek aan de toezichthouder en zorgt voor de verdere vervolgacties die kunnen voortkomen uit de melding.

Het is van belang dat bij een datalek de verantwoordelijke bestuurders geïnformeerd worden. De noodzaak hiervan neemt toe, naarmate er sprake is van een incident waarbij veel partijen betrokken zijn en veel gevoelige informatie verloren is gegaan. Ook kan het noodzakelijk zijn de bestuurders te informeren indien het incident betrekking heeft op de gemeente als geheel of er veel aandacht is in de media/pers voor een incident.

De FG beoordeelt of er sprake is van omstandigheden waarover de bestuurders en de directeur geïnformeerd dienen te worden. Indien daar sprake van is zal de FG deze informeren. Bij een crisissituatie kan gebruik worden gemaakt van crisiscommunicatie.

3. Afhandelen melding

De FG houdt een register bij van de meldingen van datalekken. In dit register verwerkt zij de interne en externe meldingen.


Melden incident
Ja
Melden incident?
Incident
Ontvangen incident
Registratie incident
Nee
Nee
1e-lijns beoordeling incident
Inbreuk beveiligingsmaatregel?
Ja
Persoonsgegevens?
Ja
2e-lijns beoordeling incident
Sprake van datalek?
Nee
Ja
Inhoudelijke beoordeling datalek
Melden datalek?
Nee
Registratie datalek, geen melding
Ja
Beoordeling datalek door FG
Melden AP?
Nee
Ja
Registratie datalek: melding AP
Melden betrokkene(n)?
Nee
Registratie datalek: melding AP, niet betrokkenen
Ja
Melden AP
Melden betrokkene(n)

4. Procedure Melden Datalekken

1. Zijn de gegevens die zijn gelekt aan te merken als persoonsgegevens?
Voorbeelden: namen, clientdata, klantnummers, (e-mail)adressen.

Nee → Je hoeft geen melding te doen

ja ↓

2. Zijn het uw 'eigen'klantgegevens die gelekt zijn?
Voorbeelden: de gegevens die een hoster opslaat, of waar een clouddienstverlener toegang tot heeft.

Nee → Je moet het lek melden aan uw klanten

ja ↓

3. Zijn er persoonsgegevens verloren geraakt of onrechtmatig verwerkt?
Voorbeelden: een verloren laptop/ telefoon, een hack, of een oud-werknemer met toegang tot persoonsgegevens. Neem bij twijfel contact met FG op.

Nee → Je hoeft geen melding te doen

ja ↓

4. Zijn een groot aantal (kwantitatief) of gevoelige gegevens (kwalitatief) gelekt?
Voorbeelden: meer dan duizend persoonsgegevens of gegevens zoals BSN, indicaties, inloggegevens. Neem bij twijfel contact met FG op.

Nee → Je hoeft geen melding te doen

ja ↓

5. U moet de toezichthouder uiterlijk 72 uur na het ontdekken van het datalek in kennis stellen van het datalek.

ja ↓

6. Heeft het datalek waarschijnlijk ongunstige gevolgen voor het privéleven van personen?
Hiervan is bijvoorbeeld sprake wanneer er gevoelige persoonsgegevens zijn gelekt of als er een gevaar is voor identiteitsfraude. Neem bij twijfel contact met FG op.

Nee → Alleen melding aan de toezichthouder

ja ↓

7. Zijn de gelekte persoonsgegevens op een manier beveiligd zodat ze niet gelezen of gebruikt kunnen worden?
Hiervan is bijvoorbeeld sprake wanneer er een goede encryptie is gebruikt. Neem bij twijfel contact met FG op.

Nee → Naast de toezichthouder ook de getroffen personen in kennis stellen van het datalek

ja ↓

8. Is de manier waarop de encryptie ongedaan gemaakt kan worden ook gelekt?

Nee → Alleen melding aan de toezichthouder

ja ↓

9. U moet naast de toezichthouder ook de getroffen personen in kennis stellen van het datalek.