Handreiking meldplicht datalekken in de eerstelijns zorg

Deel 2: Toelichting

LHV – NHG – INEEN – KNMP

Juli 2017

Inhoud

Woord vooraf

Voor u ligt een handreiking over datalekken in de eerstelijnszorg. Hiermee willen de LHV, NHG, InEen en KNMP praktische handvatten bieden aan eerstelijns zorgaanbieders.

De handreiking bestaat in feite uit drie onderdelen:

1. Een schema Eerste Hulp Bij Datalekken.
2. Een toelichting op dit schema.
3. Een overzicht van voorbeelden van datalekken.

Ad 1. Het schema Eerste Hulp Bij Datalekken bevat een overzicht van de belangrijkste drie vragen over datalekken met de antwoorden daarop:

1. Is sprake van een datalek?
2. Moet het datalek worden gemeld bij de Autoriteit Persoonsgegevens?
3. Moeten de patiënten worden geïnformeerd?

Ad 2. In deze Toelichting wordt nader uitgewerkt hoe men kan vaststellen of er sprake is van een datalek, in hoeverre het datalek moet worden gemeld bij de Autoriteit Persoonsgegevens en of patiënten ook moeten worden geïnformeerd. De Toelichting bevat naast een aantal stroomschema's ook een groot aantal vragen en antwoorden.

Ad 3. Het overzicht met 23 voorbeelden van datalekken bestaat uit een korte beschrijving van een (mogelijke) gebeurtenis, het antwoord op de vraag of deze gebeurtenis een datalek is, of dit datalek gemeld moet worden aan de AP of aan de patiënt en zo ja, wie dat zou moeten doen, en tot slot met welke maatregelen en verbeteracties een dergelijk datalek in de toekomst voorkomen kan worden.

In deze handreiking omschrijven wij een 'datalek' als "het lekken van persoonsgegevens van patiënten". Deze omschrijving omvat zowel geautomatiseerd verwerkte persoonsgegevens, als persoonsgegevens die op papier staan.

Hoewel we in deze handreiking vooral aandacht besteden aan datalekken rond patiëntengegevens, kan een datalek vanzelfsprekend ook persoonsgegevens van werknemers of andere medewerkers van een eerstelijns zorgaanbieder betreffen.

Met deze handreiking hopen wij dit ingewikkelde onderwerp wat beter toegankelijk te maken voor zorgprofessionals in de eerstelijnszorg. Wij hebben ons hierbij vooral gebaseerd op de Beleidsregels hierover van de Autoriteit Persoonsgegevens.[1] Onze handreiking kan echter niet als volledige vervanging van die Beleidsregels worden beschouwd.

Tenslotte zij vermeld dat deze handreiking tot stand is gekomen met medewerking van de KNMG.

[1] Autoriteit Persoonsgegevens, *De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). Beleidsregels voor toepassing van artikel 34a van de Wbp*. Den Haag: 8 december 2015.

Eerste Hulp bij Datalekken

Wat te doen bij een datalek in de eerstelijns zorg?

	Een datalek wil zeggen dat er vanuit of binnen uw praktijk persoonsgegevens van patiënten (data) op straat zijn gekomen, door onbevoegden zijn ingezien of verloren zijn gegaan. Sinds 1 januari 2016 is er een wet van kracht die in zulke gevallen om adequaat handelen vraagt. De eerste reactie bij een vermoeden van een datalek bestaat uit 3 stappen.		
1	**Beoordeel of er echt sprake is van een datalek**	Er is sprake van een datalek als door een inbreuk op de beveiliging, vertrouwelijke gegevens verloren kunnen zijn gegaan. Of als niet uitgesloten is dat deze door onbevoegden zijn verwerkt, binnen of buiten de beschermde omgeving van de praktijk of van de service provider.	Voorbeelden:[2] een USB-stick of pc op straat,[3] UZI-pas met pincode kwijt,[4] inbreuk door een hacker,[5] diefstal van dossiers,[6] fout van een medewerker.[7] Ook kan een andere (zorg)partij of gegevensbewerker melden dat uw gegevens zijn gelekt.[8]
2	**Beoordeel of u het lek moet melden bij de Autoriteit Persoonsgegevens (AP)**	Als er patiëntgegevens zijn gelekt, moet u dat binnen 72 uur na het bekend worden ervan melden bij de AP. Bij twijfel meldt u ook; u kunt een melding later altijd weer intrekken. Ten onrechte niet melden kan leiden tot hoge boete.	U meldt een datalek via het Meldloket Datalekken van de AP: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
3	**Beoordeel of u uw patiënten moet informeren over het lek**	Als er patiëntgegevens zijn gelekt moet u uw patiënten ook onverwijld informeren. Zij moeten zo nodig maatregelen kunnen nemen om zich te beschermen tegen de gevolgen van het datalek.	U informeert uw patiënten (individueel of in combinatie met algemene voorlichting) over de aard van de inbreuk, de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen, en de maatregelen die u de betrokkene aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken, zoals het veranderen van gebruikersnamen en wachtwoorden. De aard van de inbreuk mag u algemeen omschrijven. U vermeldt uw contactgegevens zodat de betrokkene u kan bereiken als hij of zij vragen heeft over het datalek.

[2] In de volgende voetnoten verwijzen we naar de casuïstiek in het document 'Overzicht cases datalekken'.
[3] Vgl. casus nr. 12, 13.
[4] Vgl. casus nr. 23.
[5] Vgl. casus nr. 11, 21
[6] Vgl. casus nr. 13.
[7] Vgl. casus nr. 1 t/m 7, 23.
[8] Vgl. casus nr. 10, 21.

Bijlage I. Toelichting en achtergrondinformatie

I.1 Wat is een datalek?

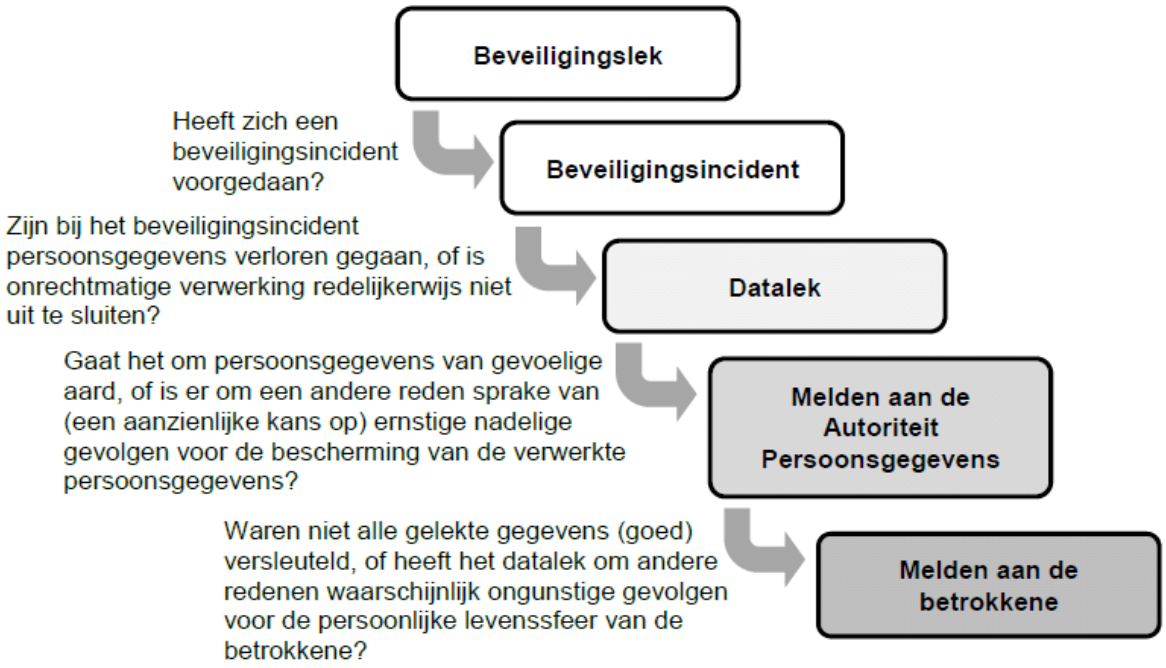
Met een 'datalek' doelen we in deze toelichting op het lekken van persoonsgegevens van patiënten. Dit kunnen zowel geautomatiseerd verwerkte persoonsgegevens zijn, maar ook persoonsgegevens die op papier staan.

Artikel 34a Wet bescherming persoonsgegevens (Wbp) omschrijft een datalek als "*een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens*".

De meldplicht datalekken is ingevoerd naar aanleiding van een aantal incidenten waarbij door een inbreuk op de beveiliging van informatiesystemen, zoals websites, persoonsgegevens zijn vrijgekomen met nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen.

Van een inbreuk op de beveiliging is sprake als de technische en organisatorische beveiligingsmaatregelen niet goed hebben gefunctioneerd. Maar de beveiliging kan ook op voldoende niveau zijn, terwijl de beveiligingsmaatregelen worden teniet gedaan of omzeild. Bijvoorbeeld wanneer een informatiesysteem dat persoonsgegevens bevat is gehackt of na diefstal van een laptop of mobiele telefoon. Daarnaast kan ook sprake zijn van menselijke fouten als iemand slordig is omgegaan met een wachtwoord dat toegang geeft tot informatiebestanden, wanneer persoonsgegevens per ongeluk worden verstuurd in een verkeerd geadresseerde envelop of e-mail, als gevoelige schriftelijke stukken als oud papier wordt aangeboden of wanneer een geheugenstick is zoek geraakt. In dergelijke gevallen is sprake van een inbreuk op de beveiligingsmaatregelen met een aanmerkelijke kans op verlies van persoonsgegevens en risico's van ongeoorloofde toegang of onrechtmatige verstrekking tot gevolg.

De Algemene Verordening Gegevensbescherming (AVG) van de EU, die op 25 mei 2018 van toepassing wordt, bevat in de artikelen 32 t/m 34 vergelijkbare bepalingen over datalekken.

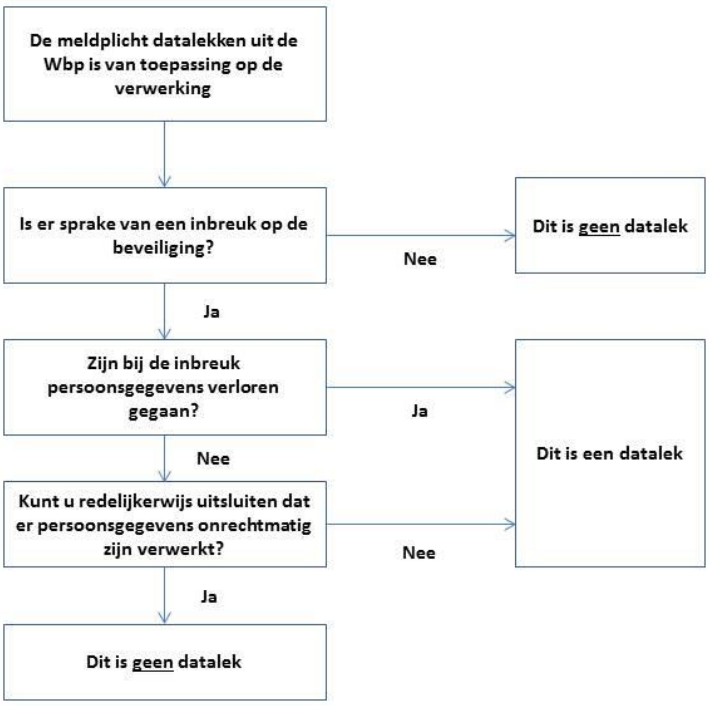


(Bron: Autoriteit Persoonsgegevens, Beleidsregels meldplicht datalekken, pag. 4-5).

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.

Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident een aanmerkelijke kans bestaat dat persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking (kennisneming) van de persoonsgegevens niet redelijkerwijs kunt uitsluiten. We kunnen ook zeggen dat in zulke gevallen de controle over de persoonsgegevens is verloren.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.



I.2 Vragen en antwoorden

- **Zijn geconstateerde tekortkomingen in de beveiliging een datalek?**
  Nee. Bij een datalek gaat het om onbedoelde toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens. Het is natuurlijk wel belangrijk dat u zorgt dat de zwakke plek in de beveiliging zo snel mogelijk wordt aangepakt.

- **Gaat het alleen om lekken bij geautomatiseerde verwerking?**
  Nee. De Wbp – en dientengevolge ook de meldplicht datalekken – is niet alleen van toepassing op de geautomatiseerde verwerking van persoonsgegevens, maar ook op gedeeltelijk of niet geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen. Met een 'bestand' wordt bedoeld een dat de gegevens deel uitmaken van een gestructureerd geheel dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
  De Wbp – en dus de meldplicht datalekken – is niet van toepassing:
  1. als geen sprake is van geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens;
  2. als geen sprake is van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om in een bestand te worden opgenomen;
  3. als persoonsgegevens alleen worden verwerkt ten behoeve van activiteiten met

uitsluitend persoonlijke of huishoudelijke doeleinden;
4. als voor een verwerking specifieke wetgeving geldt waarin de bescherming van persoonsgegevens volledig wordt geregeld (bijv. wet politiegegevens, Wet op de inlichtingen- en veiligheidsdiensten, Wet basisregistratie personen, Wet justitiële en strafvorderlijke gegevens, Kieswet);
5. als het gaat om verwerking van persoonsgegevens door de krijgsmacht in het kader van vredesoperaties. [*Bron: Beleidsregels, pag. 14*]

- **Als (versleutelde) persoonsgegevens verloren zijn, moet ik dat ook melden?**
  Persoonsgegevens kunnen op verschillende manieren verloren (lees: niet meer beschikbaar) zijn: (a) door een menselijke fout, als iemand de gegevens verwijderd of onjuist bijgewerkt heeft, (b) een systeemfout, bij een defect aan het computersysteem, of (c) in geval van een virus, als de gegevens niet meer leesbaar en/of ongewenst versleuteld zijn. Als de persoonsgegevens niet in originele staat hersteld kunnen worden, betreft het een datalek: de persoonsgegevens zijn verloren en niet meer beschikbaar en/of onjuist. Ook wanneer niet zeker gesteld kan worden dat bv. door een virus de persoonsgegevens onrechtmatig zijn verwerkt, betreft het een datalek.[9]

- **Als versleutelde gegevens zijn gelekt, moet ik dat ook melden?**
  Wanneer persoonsgegevens adequate versleuteld zijn, kan uitgesloten worden dat deze onrechtmatig zijn verwerkt (lees: ingezien). Als deze gegevens niet verloren zijn (lees: nog beschikbaar en actueel zijn), betreft het geen datalek. Dit is bijvoorbeeld het geval wanneer een gestolen of kwijtgeraakte laptop die adequate versleuteld is en de actuele persoonsgegevens nog op een andere plek staan, zoals centraal op de praktijk. De laptop bevatte op dat moment een kopie. Indien de laptop zelf alle actuele gegevens bevat en geen actuele back-up voor handen is, betreft het wel een datalek: de actuele gegevens zijn niet meer beschikbaar.

- **Geldt de meldplicht alleen voor grote lekken of voor ieder lek?**
  De omvang van een lek is niet van belang. Als de gelekte gegevens gevoelig van aard zijn (bijvoorbeeld patiëntgegevens) dan maakt het niet uit om hoeveel personen of gegevens het gaat.[10]

- **WhatsApp versleutelt ook alle berichten. Kan ik WhatsApp gebruiken voor veilige communicatie?**
  Het soort toepassing is niet relevant voor de meldplicht datalekken. Het gebruik van

[9] Bron: nieuwsbericht 3 oktober 2016: Datalek door ransomware: wat moet u doen? (Website: Autoriteit Persoonsgegevens)

[10] Onder 'gevoelige gegevens' worden verstaan: 1) 'bijzondere gegevens' als bedoeld in artikel 16 van de Wbp: persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. 2) Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens. 3) (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. 4) 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. 5) Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn). (Autoriteit Persoonsgegevens, 8 december 2015, pp. 26-27)

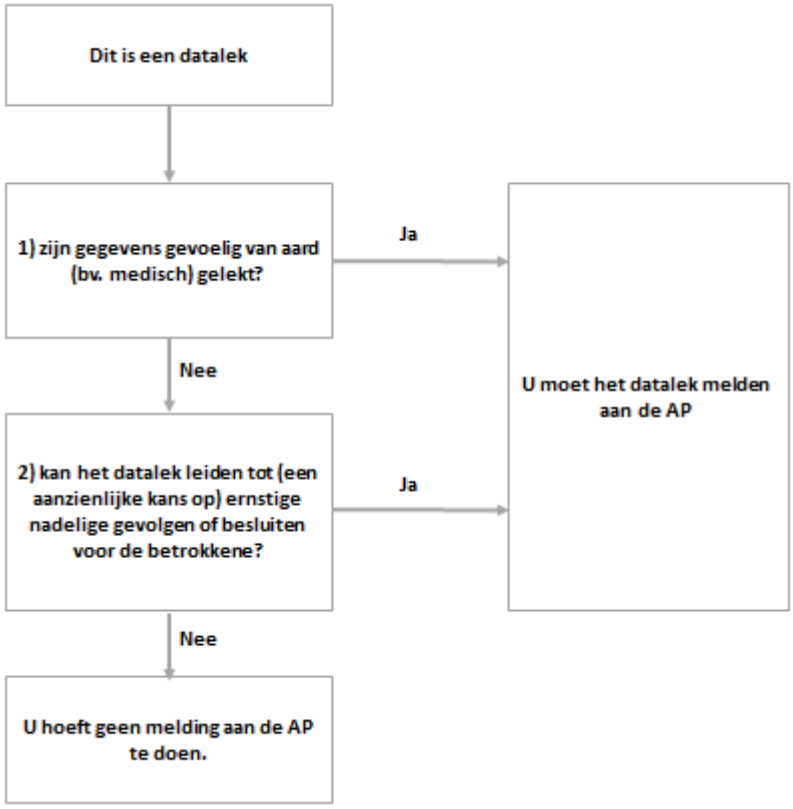
WhatsApp wordt overigens niet als 100% veilig beschouwd[11]. Aanbevolen wordt om een messenger app te gebruiken die veiliger is, zoals Signal, of een messenger app te gebruiken die speciaal is ontwikkeld voor gebruik in de gezondheidszorg, zoals op moment van schrijven Siilo, Kanta Messenger of MD Linking. (WhatsApp in de zorg: veilig of niet?, 2016)

- **Wat kan ik doen om een datalek te voorkomen?**
  Zorg dat de informatiebeveiliging in orde is. Vermijd het risico op een datalek door zoveel mogelijk processtappen zonder tot patiënten herleidbare persoonsgegevens uit te voeren. Beperk nadelige effecten door uw processtappen met een minimum aan persoonsgegevens uit te voeren. Voorkom een datalek door sterke authenticatie en goede autorisatie toe te passen waardoor persoonsgegevens niet toegankelijk zijn voor onbevoegde personen. Verhinder het ontstaan van een datalek door een samenhangend stelsel van maatregelen op te stellen.

[11] WhatsApp scoort 6 op de 7 beveiligingscriteria van de EFF Score Card sinds de invoering van End-to-End encryptie, maar wordt hiermee nog niet volledig veilig geacht aangezien de broncode niet beschikbaar is voor controle door onafhankelijke derden op de aanwezigheid van fouten, achterdeuren en structurele beveiligingsproblemen (WhatsApp in de zorg: veilig of niet?, 2016)

I.3 Melden aan de Autoriteit Persoonsgegevens?

Het onderstaande schema geeft de vragen weer die u moet beantwoorden om vast te stellen of u een specifiek datalek moet melden aan de Autoriteit Persoonsgegevens. Uitgangspunt is dat er een gebeurtenis heeft plaatsgevonden waarvan u al heeft vastgesteld dat het gaat om een datalek.



De Autoriteit Persoonsgegevens specificeert deze vragen in haar toelichting als volgt:

1. persoonsgegevens van gevoelige aard zijn gelekt. Dit betekent dat als persoonsgegevens over iemands gezondheid, zoals gegevens uit een medisch dossier, zijn gelekt, dit altijd gemeld moet worden aan de Autoriteit Persoonsgegevens. Dit geldt bijvoorbeeld ook voor gebruikersnamen, wachtwoorden en andere inloggegevens en voor gegevens die iemand kunnen identificeren, zoals kopieën van identiteitsbewijzen en het burgerservicenummer (BSN).

2. de aard en omvang van het datalek leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de gegevens over de patiënt. Hiervan is sprake als persoonsgegevens van gevoelige aard zijn gelekt (zie hierboven onder punt 1), als per persoon veel persoonsgegevens zijn gelekt, als er ingrijpende beslissingen genomen worden op basis van de gegevens (met financiële gevolgen voor de patiënt), of als de persoonsgegevens binnen een keten worden gedeeld. Dit geldt ook voor gegevens van personen uit zogeheten ‘kwetsbare groepen’ (bewoners van blijf-van-mijn-lijf-huis, kinderen en mensen met een verstandelijke handicap.

I.4 Vragen en antwoorden

- **Wie moet er melden aan de Autoriteit Persoonsgegevens?**
  De Verantwoordelijke voor de verwerking van de persoonsgegevens is verantwoordelijk voor het melden van een datalek. Dit kan een individuele apotheker of huisarts zijn, maar ook een bestuur van een zorgpraktijk. Wanneer het datalek betrekking heeft op zorg die wordt verleend in georganiseerd verband (bijvoorbeeld door een Huisartsenpost, een Zorggroep of een Gezondheidscentrum) dan is (het bestuur van) die organisatie de aangewezen partij om dit te melden bij de Autoriteit Persoonsgegevens.

- **Waarom moet ik melden aan de Autoriteit Persoonsgegevens?**
  Met de meldplicht aan de Autoriteit Persoonsgegevens word beoogd het toezicht op potentieel ernstige datalekken te ondersteunen. Het informeren van de Autoriteit Persoonsgegevens is nodig opdat deze kan beoordelen of een onderzoek of het geven van aanwijzingen nodig is.

- **Wanneer moet ik een datalek melden aan de Autoriteit Persoonsgegevens?**
  U bent verplicht een datalek te melden aan de Autoriteit Persoonsgegevens als 1) patiëntgegevens of andere 'gevoelige gegevens' zijn gelekt, verloren zijn gegaan of als onrechtmatige verwerking zoals kennisneming van de gegevens niet valt uit te sluiten of 2) als het andere persoonsgegevens betreft en de aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen (bijvoorbeeld: door een technische storing zijn medische gegevens ingezien door onbevoegden). U moet binnen 72 uur na het bekend worden van het lek, dit melden bij de Autoriteit Persoonsgegevens. Bij twijfel meldt u ook; u kunt een melding later altijd weer intrekken. Ten onrechte niet melden kan leiden tot hoge boetes.

- **Hoe moet ik een datalek melden aan de Autoriteit Persoonsgegevens ?**
  Melden is mogelijk via een webformulier of via een papieren formulier. Melden doet u via het Meldloket Datalekken van de Autoriteit Persoonsgegevens. Zie:
  https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
  Zie ook de website van de Autoriteit Persoonsgegevens voor meer informatie:
  https://www.autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

- **Wat moet ik melden aan de Autoriteit Persoonsgegevens?**
  Bij een melding wordt u gevraagd informatie te verstrekken over:

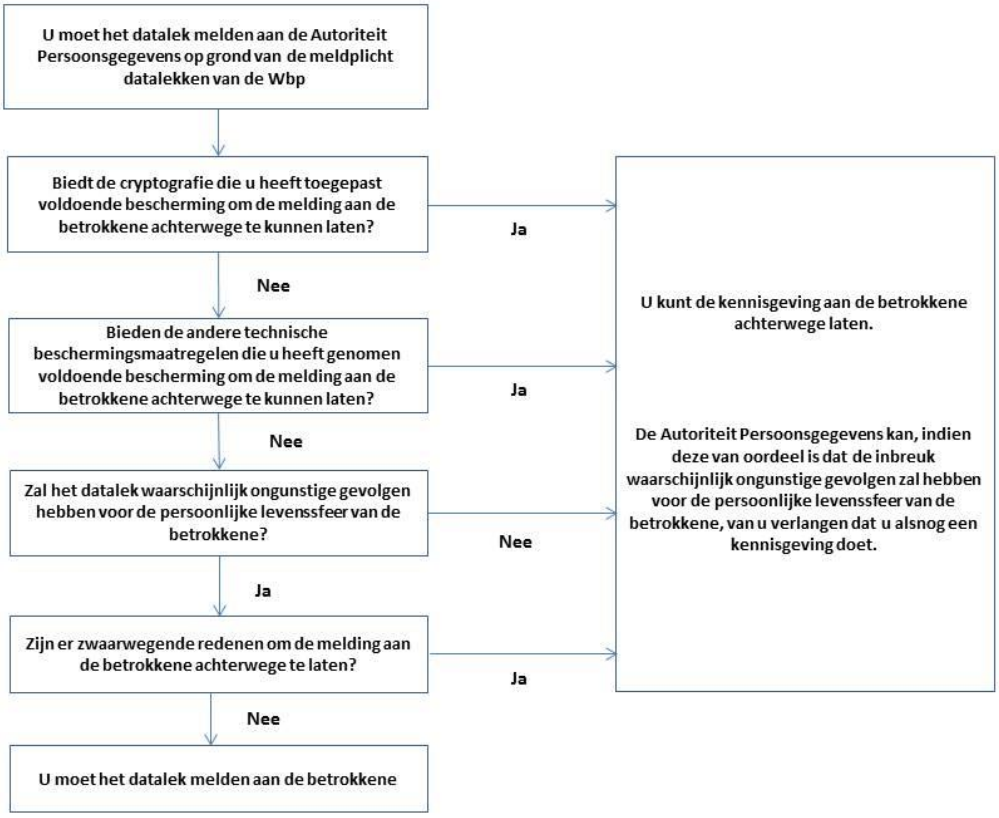
  - de aard van de melding (eerste melding of vervolg op een eerdere melding),
  - het wettelijk kader voor deze melding (Wet bescherming persoonsgegevens),
  - algemene informatie en contactgegevens,
  - gegevens over het datalek,
  - naar aanleiding van het datalek getroffen vervolgacties,
  - informatie over het inlichten van patiënten,
  - getroffen technische maatregelen,
  - internationale aspecten
  - of er nog een vervolgmelding zal volgen.

- **Welke informatie moet ik melden aan de Autoriteit Persoonsgegevens?**
  Melden doet u via het Meldloket Datalekken van de Autoriteit Persoonsgegevens . Zie: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
  Zie ook de Bijlage bij de Beleidsregels of http://www.privacyindezorg.nl/datalekken.html.

- **Wat doet de Autoriteit Persoonsgegevens met mijn melding?**
  Na de melding ontvangt u een ontvangstbevestiging van de Autoriteit Persoonsgegevens. Als daar aanleiding voor is neemt de Autoriteit Persoonsgegevens contact met u op om te verifiëren dat de gedane melding daadwerkelijk van u afkomstig is en om eventueel inhoudelijke vragen over de melding te stellen. De Autoriteit Persoonsgegevens ziet er op toe dat de betrokken personen (patiënten, cliënten) zo nodig worden geïnformeerd. Als u dat ten onrechte niet heeft gedaan kan de Autoriteit Persoonsgegevens van u verlangen dat u dat alsnog doet. Blijft u dan nog in gebreke dan kan de Autoriteit Persoonsgegevens u bestraffen met een bestuurlijke boete. Ook kan de melding aanleiding zijn voor de Autoriteit Persoonsgegevens om een onderzoek in te stellen naar de informatiebeveiliging. Alle datalekmeldingen worden in een register vastgelegd. Dit register is niet openbaar.

I.5 Melden aan de patiënt?

Het onderstaande schema geeft de vragen weer die u moet beantwoorden om vast te stellen of u een specifiek datalek moet melden aan uw patiënten. De paragraafnummers verwijzen naar de paragrafen in de Beleidsregels van de Autoriteit Persoonsgegevens.



De Autoriteit Persoonsgegevens stelt in de beleidsregels over de meldplicht datalekken dat u er van uit moet gaan dat u een datalek van persoonsgegevens van gevoelige aard, zoals patiëntgegevens, niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokken patiënten (Beleidsregels, par. 7.4).

Het informeren van patiënten mag achterwege worden gelaten als daar zwaarwegende redenen voor zijn. Dat geldt bijvoorbeeld als gegevens zijn gelekt over medische en/of psychosociale hulpvragen die kinderen buiten medeweten van hun ouders hebben gesteld. Door informatie over een datalek te verstrekken aan de ouders zouden die langs deze weg op de hoogte kunnen raken van de hulpvraag van hun kind. Om dat te voorkomen mag de informatie aan de betrokkene (de ouders in dit geval) achterwege blijven. Het datalek moet dan overigens wel gemeld worden aan de Autoriteit Persoonsgegevens.

Indien u passende technische beschermingsmaatregelen heeft genomen, zoals versleuteling van de gegevens (cryptografie), waardoor de persoonsgegevens die het betreft onbegrijpelijk of

ontoegankelijk zijn voor anderen die geen recht hebben op kennisname van de gegevens, dan mag u de melding aan de betrokkene achterwege laten (artikel 34a, zesde lid, Wbp).

In eerste instantie moet u zelf beoordelen of de versleuteling sterk genoeg is en juist wordt uitgevoerd. Dit moet u periodiek doen, omdat deze techniek zich voortdurend ontwikkeld. Volgens de Europese verordening 611/2013 is de versleuteling adequaat als de gegevens:

- op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of
- zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.

Met ‘andere technische beschermingsmaatregelen’ wordt gedoeld op ‘remote wiping’, oftewel het op afstand wissen van de gegevens die op een apparaat staan. Ook ‘pseudonimisering’ is zo’n andere maatregel. Daarmee kan worden voorkomen dat persoonsgegevens aan een identiteit van een persoon kunnen worden gekoppeld. In beide gevallen moet wel worden vastgesteld dat de gegevens voor de onrechtmatige ontvanger ‘onbegrijpelijk of ontoegankelijk’ zijn.

I.6 Vragen en antwoorden

- **Moet ik een datalek melden aan de patiënt(en)?**
  Als niet alle gelekte gegevens (goed) versleuteld waren, of het datalek om andere redenen waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene. Daarbij moet u bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kunt u er in principe van uit gaan dat u het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.

- **Waarom moet ik een datalek melden aan de patiënt(en)?**
  U moet een datalek melden aan de patiënt(en) om hen op de hoogte te stellen van de feitelijke situatie met betrekking tot hun persoonsgegevens en de gevolgen die dat voor hun belangen heeft. Aldus kunnen de patiënten nadere informatie opvragen of beslissen of zij gebruik willen maken van hun recht op inzage, correctie of afscherming. Door de kennisgeving aan de patiënt(en) kunnen zij alert zijn op de mogelijke gevolgen van het datalek. Bovendien kunnen zij dan maatregelen nemen, zoals het veranderen van hun wachtwoord.

- **Wanneer moet ik een datalek melden aan de patiënt(en)?**
  In de Wet bescherming persoonsgegevens staat dat u het datalek “onverwijld” moet melden aan “de betrokkenen”, zoals uw patiënten. Na het ontdekken van het datalek mag u enige

tijd nemen voor nader onderzoek zodat u de patiënten op een behoorlijke en zorgvuldige manier kunt informeren. Wel moet u er rekening mee houden dat de patiënten naar aanleiding van uw melding mogelijk maatregelen moeten nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder u de betrokkenen daarover informeert, hoe eerder zij in actie kunnen komen. Ook als u niet verplicht bent om een datalek te melden aan patiënten, kunt u ervoor kiezen om dat toch te doen. Dit kan het vertrouwen in uw organisatie vergroten.

- **Hoe beslis ik op welke wijze ik een datalek meld aan de patiënt(en)?**
  Uitgangspunt hierbij is dat de betrokkene op basis van zijn/haar impact voldoende wordt geïnformeerd, waarbij rekening gehouden mag worden met de gelieerde kosten. Indien u beschikt over contactgegevens, bent u wellicht in staat om een algemene (/of, afhankelijk van de impact een persoonlijke) brief of e-mail naar elke individu te sturen. In geval van lage impact en een grote omvang, zoals merendeel van uw patiënten, kan een algemeen bericht ook volstaan: bijvoorbeeld in de wachtkamer of bij de balie, een publicatie in een plaatselijk dagblad, of een vermelding op de website. In beide gevallen kan bv. op basis van de impact (bij een kleine omvang) doorverwezen worden naar een informatiepunt met telefoonnummer of e-mail voor het stellen van vragen, of (bij een grote omvang) een informatiebijeenkomst waar patiënten naar toe kunnen. Met uw melding moet u in ieder geval zo veel mogelijk betrokkenen bereiken met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken.

- **Welke informatie over een datalek moet ik melden aan de patiënt?**
  In de kennisgeving aan de betrokkene vermeldt u in ieder geval:
  1) wat er aan de hand is (de aard van het datalek), meestal is een algemene omschrijving van de situatie voldoende,
  2) waar ze terecht kunnen met vragen, zowel uw eigen contactgegevens (telefoonnummer, e-mailadres, chats) als die van de betrokken instanties;
  3) wat de betrokkenen zelf kunnen doen om de negatieve gevolgen van de inbreuk te beperken (bijvoorbeeld gebruikersnaam en wachtwoord wijzigen wanneer dat samenhangt met het datalek).
  Het staat u vrij om meer informatie toe te voegen aan de kennisgeving, maar dit is niet verplicht.

I.7 Wat meldt u aan patiënten?

Een melding aan patiënten dient ten minste de volgende onderdelen te bevatten.[12]

1. Wat is er aan de hand?
Leg in duidelijke en eenvoudige taal uit wat er aan de hand is en wat de mogelijk gevolgen voor hen kunnen zijn (eventueel gefaseerd, voor zover de informatie nog niet voorhanden is):
- om wat voor soort datalek gaat het: zijn er gegevens in handen van onbevoegden gekomen, verloren gegaan, of iets anders?
- wat is er precies gebeurd?
- staat het vast dat er gegevens zijn gelekt: is het zeker dat “mijn” gegevens zijn gelekt?
- zo nee, hoe waarschijnlijk of onwaarschijnlijk is dat dan toch het geval?
- wat voor soort gegevens zijn er gelekt: “gewone” (NAW) gegevens of “gevoelige” gegevens (patiëntgegevens, BSN)?
- van hoeveel personen zijn gegevens gelekt (bij benadering)?
- uit welke bestanden zijn gegevens gelekt?
- wat voor misbruik zou iemand van de gelekte gegevens kunnen maken?
- hoe groot is het risico dat dit ook echt gebeurt?
- welke maatregelen zijn getroffen om de eventuele nadelige gevolgen te beperken?
- welke maatregelen zijn er getroffen of worden voorgenomen om het datalek te verhelpen?

2. Waar kan ik terecht met vragen?
Als er een reëel risico op misbruik van de gelekte gegevens bestaat, zullen sommige patiënten vragen hebben of zich zorgen maken. Informeer de patiënten daarom waar ze met hun zorgen en vragen terecht kunnen. Kanaliseer alle vragen via een regulier contactpunt (loket) maar voor verschillende methoden (e-mail, telefoon, chat). Laat u het over aan de dokters- of apothekersassistente, zorg er dan voor dat deze voldoende is geïnstrueerd, ook over waar men terecht kan met moeilijke vragen.

3. Wat kan ik zelf doen?
Licht eerst toe welke maatregelen uw organisatie reeds heeft genomen om de gevolgen van het datalek te beperken. Informeer de patiënten vervolgens wat zij in aanvulling daarop zelf kunnen doen, zoals het wijzigen van een wachtwoord (eventueel ook in andere systemen).

[12] Bron: J. Hutter e.a., *Grip op datalekken. Handreiking voor het beheersen van datalekrisico’s.* Wolters Kluwer, 2015, pag. 82 e.v. Vgl. ook art. 33 en 34 Verordening (EU) 2016/679 (algemene verordening gegevensbescherming).

Bijlage II. Voorbereiden op een datalek

Zorgorganisaties, ook in de eerstelijns zorg, kunnen en moeten hun processen aanpassen naar aanleiding van de meldplicht datalekken. Daardoor kunnen veel problemen worden voorkomen. Datalekken kunnen optreden als gevolg van tekortkomingen op het gebied van menselijk gedrag, organisatie en ICT. Organisaties kunnen verschillende maatregelen treffen om zich voor te bereiden op een datalek. De volgende maatregelen helpen de organisatie om snel en adequaat te kunnen reageren:

- Zorg voor een goede beveiliging van de persoonsgegevens die je verwerkt. Dit geldt zowel in de ICT-omgeving als in procedures voor omgang met persoonsgegevens binnen de organisatie. Denk hierbij aan het implementeren van de norm NEN-7510, maar ook bijvoorbeeld aan het opstellen van heldere procedures voor het verzenden, archiveren of vernietigen van documenten die privacygevoelige informatie bevatten.
- Stel een persoon aan binnen de organisatie die beveiligingsincidenten en potentiële datalekken beoordeelt en die zo nodig meldt bij de Autoriteit Persoonsgegevens. Zorg ervoor dat de betreffende medewerker voldoende is toegerust voor deze taak en biedt zo nodig scholing aan.
- Zorg voor adequaat incidentenbeheer waarbij zowel incidenten die zijn gemeld bij de AP als incidenten die niet zijn gemeld zorgvuldig worden gedocumenteerd, inclusief de afweging die tot de betreffende keuze heeft geleid.
- Richt een procedure in voor het informeren van betrokkenen bij een datalek. De meldplicht datalekken schrijft voor dat betrokken personen of patiënten moeten worden geïnformeerd als het aannemelijk is dat een datalek schade voor hen oplevert. Uitgangspunt is dat als er patiëntgegevens zijn gelekt, de patiënten altijd daarover moeten worden geïnformeerd.
- Denk na over hoe om te gaan met signalen over mogelijke datalekken van buitenaf of uit de media en leg dit eventueel vast in een communicatieplan.
- Controleer bestaande overeenkomsten met bewerkers. De NVZ-modelbewerkersovereenkomst kan hierbij als voorbeeld dienen. Maak aanvullende afspraken met databewerkers over wie wat doet wanneer er een datalek wordt geconstateerd.

Voorbeelddocumenten (van een ziekenhuisorganisatie) zijn te vinden op:
http://www.privacyindezorg.nl/datalekken.html

Bijlage III. Wat doet de Autoriteit Persoonsgegevens?

Na de melding

Na een melding aan de Autoriteit Persoonsgegevens slaat deze uw melding op in een register met alle ontvangen meldingen over datalekken. Dit register is niet openbaar. De Autoriteit Persoonsgegevens kan contact met u opnemen als er inhoudelijke vragen zijn over uw melding. Heeft u de betrokkenen niet geïnformeerd over het datalek? Maar is dat volgens de wet wel noodzakelijk? Dan kan de Autoriteit Persoonsgegevens u vragen om dat alsnog te doen. Uw datalekmelding kan, eventueel in combinatie met andere meldingen, ook aanleiding zijn voor de Autoriteit Persoonsgegevens om een onderzoek te starten naar de naleving van de privacywetgeving.

Boete

De Autoriteit Persoonsgegevens kan bij overtreding van de meldplicht datalekken uit de Wet bescherming persoonsgegevens een boete opleggen van maximaal 820.000 euro. Voor overtreding van de meldplicht datalekken uit de Telecommunicatiewet kan de Autoriteit Persoonsgegevens een boete opleggen van maximaal 900.000 euro. In de Boetebeleidsregels Autoriteit Persoonsgegevens 2016 staat hoe de Autoriteit Persoonsgegevens de hoogte van boetes bepaalt. Is de overtreding niet opzettelijk gepleegd? En is er geen sprake van ernstig verwijtbare nalatigheid? Dan legt de Autoriteit Persoonsgegevens eerst een bindende aanwijzing op. Daarna legt de Autoriteit Persoonsgegevens eventueel een boete op. Bij het opleggen van een boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Zo'n omstandigheid is bijvoorbeeld dat de gelekte gegevens niet door derden zijn ingezien. Sinds 1 januari 2016 heeft de Autoriteit Persoonsgegevens een boetebevoegdheid.

Bindende aanwijzing

De boetebandbreedte voor het ten onrechte niet melden van een datalek aan de Autoriteit Persoonsgegevens (art. 34a, eerste lid, Wbp) ligt tussen de € 120.000 en € 500.000. Is het datalek niet opzettelijk niet gemeld of is geen sprake van ernstig verwijtbare nalatigheid, dan gaat eerst een bindende aanwijzing vooraf aan het opleggen van een boete door de Autoriteit Persoonsgegevens. In de bindende aanwijzing zal de Autoriteit Persoonsgegevens ter concretisering van de wettelijke norm moeten aangeven welke gedraging op grond van de Wbp van de overtreder wordt verwacht en hem zo mogelijk moeten opdragen om de overtreding geheel of gedeeltelijk te herstellen. De Autoriteit Persoonsgegevens kan daarbij de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd. Indien de aanwijzing niet wordt opgevolgd, is de Autoriteit Persoonsgegevens reeds om die reden bevoegd een boete op te leggen.

Relevante factoren

Bij het bepalen van de hoogte van de boete houdt de Autoriteit Persoonsgegevens rekening met de ernst van de overtreding. De Autoriteit Persoonsgegevens laat de ernst van de overtreding mede afhangen van een aantal factoren:

- de aard en omvang van de overtreding;

- de duur van de overtreding;
- de impact van de overtreding op (de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor) de betrokkenen en/of de maatschappij.

De Autoriteit Persoonsgegevens houdt ook rekening met de mate waarin de overtreding aan de overtreder kan worden verweten. De Autoriteit Persoonsgegevens houdt zo nodig ook rekening met de omstandigheden waaronder de overtreding is gepleegd en de (financiële) omstandigheden waarin de overtreder verkeert.

Bijlage IV. Bibliografie

Autoriteit Persoonsgegevens, *De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). Beleidsregels voor toepassing van artikel 34a van de Wbp*. Den Haag, 8 december 2015.

J. Hutter, S. Katus, J. Terstegge, K. Versmissen, *Grip op datalekken. Handreiking voor het beheersen van datalekrisico's*. Wolters Kluwer, 2015.

RPCG, Privacy in de zorg – datalekken: http://www.privacyindezorg.nl/datalekken.html

Ir. H. Candel, mr. dr. S. Nouwt, 'Help, een datalek!'. *Privacy & Informatie* 2016/3.

Mr. C.M.M. Zwinkels, 'De meldplicht datalekken: de bewerkers-overeenkomst.' *Privacy & Informatie* 2016/49.

dr. S. Nouwt, 'WhatsApp in de zorg: veilig of niet?' *Tijdschrift zorg en recht in de praktijk*, SDU, 2016/6