Ir. H. Candel en mr. dr. S. Nouwt[*]

Help, een datalek!

Een procedure voor het omgaan met datalekken

3

Trefwoorden:
meldplicht datalekken

Op 1 januari 2016 is een wijziging van de Wet bescherming persoonsgegevens (hierna: Wbp) in werking getreden, die onder andere een meldplicht regelt voor datalekken. In het Elisabeth-TweeSteden Ziekenhuis te Tilburg (hierna: ETZ) is een procedure ontwikkeld die medewerkers van de instelling een praktisch handvat biedt hoe te handelen bij een (vermoeden van een) datalek. Deze Procedure Meldplicht Datalekken is vastgesteld in de vergadering van de raad van bestuur (hierna: RvB) van het ETZ d.d. 7 december 2015, in diens hoedanigheid van verantwoordelijke voor de gegevensverwerking. Hierna volgt een beschrijving van die procedure. Deze procedure kan als voorbeeld dienen voor andere organisaties.[1]

Doel van de procedure

De meldplicht datalekken houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken onverwijld moeten melden aan de Autoriteit Persoonsgegevens (hierna: AP) en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.

De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt, moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt.

De procedure die het ETZ heeft ontwikkeld, beschrijft hoe te handelen binnen het ETZ indien er sprake is van een datalek of wanneer een datalek vermoed wordt. De procedure strekt zich ook uit tot een datalek dat bij een derde is ontstaan, bijvoorbeeld bij een bewerker van persoonsgegevens van het ETZ. De meldplicht is immers ook dan van toepassing op het ETZ.

De procedure is mede gebaseerd op de beleidsregels van de AP inzake de Meldplicht datalekken in de Wbp.[2]

Het ETZ heeft, zoals ook andere organisaties, nog geen ervaring kunnen opdoen met deze procedure op grond van gemelde datalekken. Daar waar nodig zal de procedure in de toekomst dan ook kunnen worden aangepast op grond van de verkregen ervaring door het ETZ. Om die reden behoudt de raad van bestuur de vrijheid om per gemeld datalek te beoordelen of de procedure gevolgd kan worden, dan wel afwijking van deze procedure gerechtvaardigd is.

Het doel van deze procedure is vast te leggen welke stappen genomen moeten worden door het ETZ bij een vermoeden of kennisneming van een incident dat (mogelijk) aangemerkt kan worden als een datalek.

Het volgende resultaat wordt hiermee nagestreefd:

- het steeds volgen van een eenduidige procedure;
- het zorgvuldig waarborgen van de belangen van het ETZ, het individu dan wel een ander bedrijf dat betrokken is bij het incident, zijnde (mogelijk) datalek;
- het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident;
- het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen;
- het realiseren van een voldoende en eenduidige interne en op verzoek externe verantwoording over de afhandeling van een incident, zijnde (mogelijk) datalek.

In de procedurebeschrijving zijn de te doorlopen stappen verwoord.

Definities

In de gewijzigde Wbp en in de onderhavige procedure komen enkele nieuwe begrippen voor die in de procedure nader worden omschreven. De volgende zijn daarvan de belangrijkste.

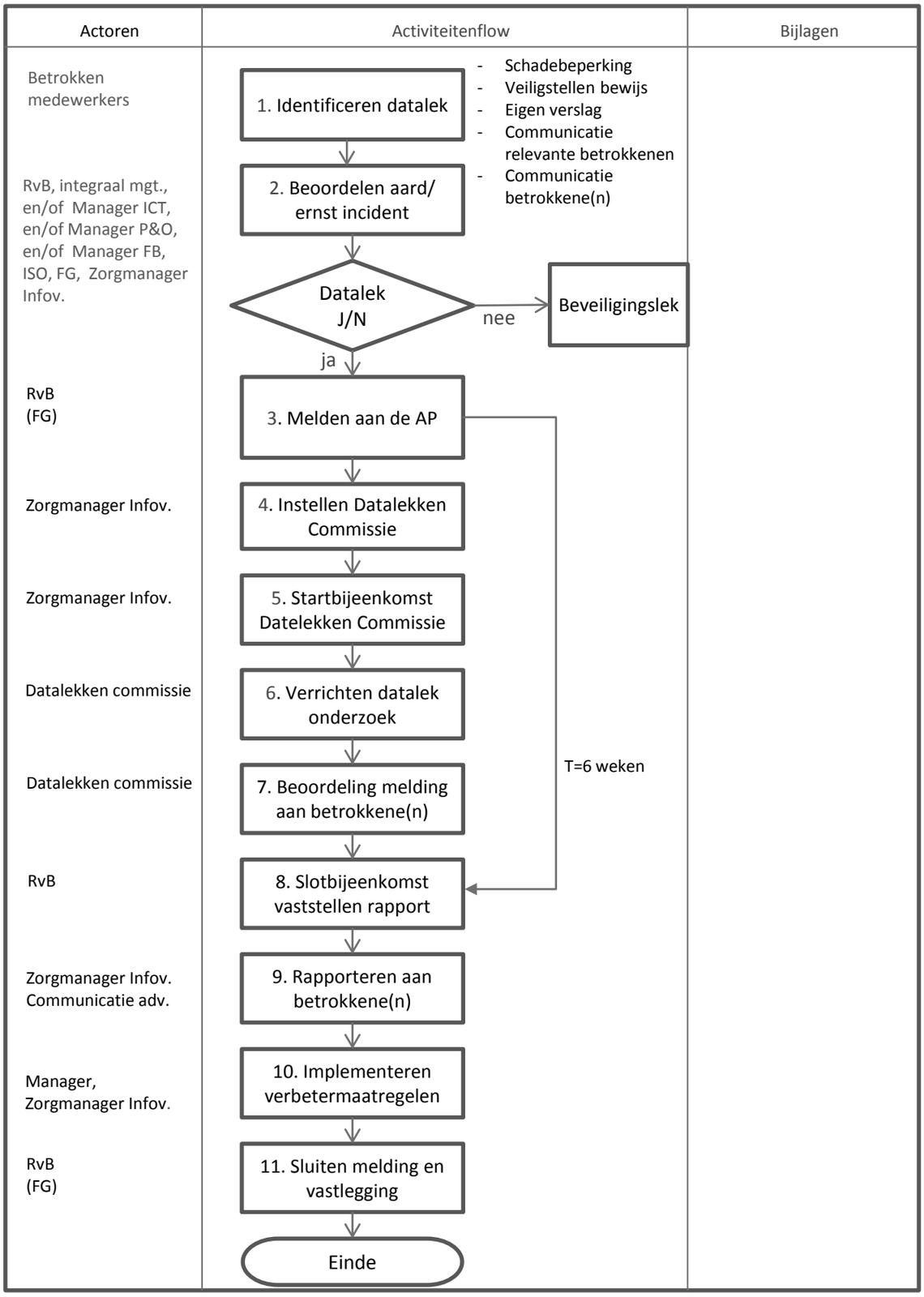
De *Autoriteit Persoonsgegevens* is de nieuwe naam van het College bescherming persoonsgegevens (CBP) sinds 1 januari 2016.

---

* **Hans Candel is informatiemanager in het Elisabeth-TweeSteden Ziekenhuis, locatie Tilburg. Sjaak Nouwt is privacyadviseur, adviseur gezondheidsrecht bij de artsenfederatie KNMG en hoofdredacteur van *P&I*. Beide zijn als lid, respectievelijk voorzitter verbonden aan de Regionale Privacy Commissie voor de Gezondheidszorg (RPCG, zie: www.privacyindezorg.nl).**

1 De procedure met bijlagen is beschikbaar op de website www.privacyindezorg.nl.

2 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.



Een *beveiligingslek* is een *inbreuk* op de beveiliging (zoals bedoeld in artikel 34a lid 1 Wbp) waarbij persoonsgegevens *niet* worden blootgesteld aan verlies of onrechtmatige verwerking; er is dan geen sprake van een *datalek*.

Een *datalek* is een *inbreuk* op de beveiliging (zoals bedoeld in artikel 34a lid 1 Wbp) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 13 Wbp) bescherming moesten bieden.

De *Datalekken Commissie* is een door de Zorgmanager Informatieveiligheid tijdelijk ingestelde onderzoekscom-

missie, die zorgdraagt voor een onderzoek en over de uitkomsten rapporteert aan de raad van bestuur.

Een *incident* is een mogelijk beveiligingsincident, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder datalek is een incident, niet ieder incident is een datalek.

De *Zorgmanager Informatiebeleid* is een zorgmanager (lijnmanager primair proces) die vanuit de portefeuille Informatieveiligheid belast is met de interne coördinatie van de procedure meldplicht datalekken.

Het processchema

Ten behoeve van het totaaloverzicht van de procedure is een processchema opgesteld. Dat schema is hiervóór opgenomen. Vervolgens is specifieke informatie per processtap over de te verrichten activiteiten en bijbehorende verantwoordelijkheden en bevoegdheden in de procedure uitgewerkt. Die informatie geven wij in aansluiting op het processchema weer. De nummering van de processtappen komt overeen met die in het processchema.

De processtappen

1 *Identificeren van een datalek*

De medewerker die een (mogelijk) datalek constateert, meldt dit incident per omgaande bij zijn organisatorisch hoofd. Vervolgens meldt dit hoofd het incident per omgaande aan het integraal management of aan een daarmee gelijkgestelde manager. Deze zorgt ervoor dat de Zorgmanager Informatieveiligheid (of diens plaatsvervanger) onmiddellijk wordt geïnformeerd. Iedere medewerker is te allen tijde bevoegd zelfstandig een melding te doen aan de Zorgmanager Informatieveiligheid, dus ook bij gebreke van een melding aan de Zorgmanager Informatieveiligheid anderszins. Ook (de medewerker van) een bewerker kan een datalek constateren en daarvan melding doen bij diens opdrachtgever in het ETZ.

Hierna wordt de procedure meldplicht datalekken echt gestart.

2 *Beoordeling aard/ernst incident; datalek ja/nee*

Nadat de Zorgmanager Informatieveiligheid over een mogelijk datalek is geïnformeerd, draagt deze, in samenspraak met de Functionaris Gegevensbescherming (hierna: FG), zo spoedig mogelijk zorg voor het verzamelen van volledige en juiste informatie. Hiervoor wordt gebruikgemaakt van het 'Formulier voor melding datalek'. Dit formulier maakt als bijlage 1 deel uit van de beschreven procedure. Het formulier bevat de vragen die door de AP zijn opgenomen als bijlage 'Gegevens in de melding' bij de Beleidsregels meldplicht datalekken.[3]

Op basis van de verkregen informatie en bij vermoeden van een datalek wordt in overleg tussen de RvB, integraal management of daarmee gelijkgestelde manager en/of manager ICT en/of manager P&O en/of manager Facilitair bedrijf, Zorgmanager Informatieveiligheid, FG en Information Security Officer (hierna: ISO) zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een datalek. In dit overleg kan tevens worden beoordeeld of er per direct maatregelen genomen moeten worden om de schade te beperken, zoals het doen van een (voorlopige) melding aan betrokkenen. Zo nodig kan advies gevraagd worden aan de juridisch adviseur en aan de communicatieadviseur. Ook kan worden beoordeeld of van het datalek melding of aangifte zal worden gedaan bij de politie in geval van vermoeden van een strafbaar feit (zie ook hierna onder punt 3).

De beoordeling of er sprake is van een incident dat gemeld moet worden aan de AP kan tot stand komen met behulp van de schema's te vinden in de beleidsregels 'Meldplicht datalekken in de Wet bescherming persoonsgegevens' van de AP (bijlage 2 bij de procedure). Bij die beoordeling spelen onder andere een rol:

- is er sprake van *verlies* van persoonsgegevens? dit houdt in dat het ETZ deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan;
- is er sprake van *onrechtmatige verwerking* van persoonsgegevens? hieronder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens, of een niet-geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan;
- is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging?;
- kan redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid?;
- zijn er persoonsgegevens van gevoelige aard gelekt? Gevoelige persoonsgegevens zijn:
  - bijzondere persoonsgegevens conform artikel 16 Wbp;
  - gegevens over de financiële of economische situatie van de betrokkene;
  - gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
  - gebruikersnamen, wachtwoorden en andere inloggegevens;
  - gegevens die kunnen worden gebruikt voor (identiteits)fraude;
- leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens? hierbij worden factoren betrokken zoals:

3 De bijlagen bij de beschreven procedure zijn eveneens beschikbaar op www.privacyindezorg.nl > dossier informatiebeveiliging > meldplicht datalekken.

- de omvang van de verwerking; gaat het om veel persoonsgegevens per persoon, en/of om gegevens van grote groepen betrokkenen?;
- de impact van verlies of onrechtmatige verwerking;
- het delen van de persoonsgegevens binnen (zorg)ketens; dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten kunnen optreden;
- betrokkenheid van kwetsbare groepen; denk aan verstandelijk gehandicapten.

In het geval dat er geoordeeld wordt dat sprake is van een (mogelijk) datalek, wordt tevens het communicatietraject richting betrokkene(n) en – indien van toepassing – de bewerker besproken. In het geval dat het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. Een melding aan de AP is dan niet aan de orde. Wel kan in het overleg besloten worden dat het zinvol is om het beveiligingslek te onderzoeken om herhaling of een datalek in de toekomst te voorkomen.

3 *Melden aan de Autoriteit Persoonsgegevens*

De RvB (of op diens verzoek: de FG) verzorgt de tijdige elektronische melding bij de AP volgens het online meldingsformulier van de AP.[4] Dit met inachtneming van de richtlijnen van de AP terzake. Tijdige melding wil zeggen: onverwijld, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. In samenspraak met de FG draagt de Zorgmanager Informatieveiligheid zorg voor de volledige en juiste informatie zoals opgenomen in bijlage 1 'Formulier voor melding datalek' aan de RvB. Op grond van dat formulier zal feitelijk gemeld worden. De RvB (of op diens verzoek: de FG) fungeert als contactpersoon voor de communicatie met de AP. Dit geldt ook ingeval nog niet duidelijk is of het incident een datalek is. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het incident de melding aan te vullen dan wel in te trekken. Na de melding van het datalek zal de AP een ontvangstbevestiging sturen. Alleen indien de melding daartoe aanleiding geeft, zal de AP contact opnemen met de melder.

De RvB is eindverantwoordelijk voor de melding aan de AP, maar ook anderen binnen ETZ hebben een rol in deze procedure. De Zorgmanager Informatieveiligheid is gedelegeerd regievoerder over de interne afhandeling van het (mogelijke) datalek in al zijn facetten. De FG is regievoerder over de externe afhandeling met de AP, de betrokkenen en de bewerker. Het direct betrokken (integraal) management zorgt ervoor dat de bij het incident betrokken medewerkers worden geïnformeerd. Het direct betrokken (integraal) management zorgt er ook voor dat de betrokken medewerkers bij het incident, het mogelijke datalek, zo snel mogelijk een eigen verslag opstellen over de toedracht van het incident. Deze schriftelijke informatie wordt aan de RvB en Zorgmanager Informatieveiligheid verstrekt ten behoeve van de leden van de Datalekken Commissie (zie hierna onder punt 4) en het in te richten 'Dossier datalekken'.

Bij een datalek als gevolg van een (niet-ethische) hack is sprake van een strafbaar feit ('Computervredebreuk', artikel 138ab Wetboek van Strafrecht). Ook dan is van belang wat de aard van de gelekte persoonsgegevens is en wat de risico's van misbruik voor de betrokkene(n) zijn. Bij een dergelijke hack ligt naast melding bij de AP, ook melding of aangifte bij de politie in de rede in verband met de opsporing van de daders. Een aangifte bij de politie loopt altijd via de contactfunctionaris voor de politie bij het ETZ.

4 *De Datalekken Commissie*

Na de melding aan de AP gaat de Zorgmanager Informatieveiligheid over tot het samenstellen van een Datalekken Commissie om verdergaand onderzoek te verrichten. Deze commissie bestaat uit ten minste drie leden. Betrokkenen bij het incident, dan wel de afdeling waar het incident heeft plaatsgevonden, kunnen niet participeren in de commissie. Bij de samenstelling van de Datalekken Commissie wordt rekening gehouden met de aard van het incident. De Zorgmanager Informatieveiligheid faciliteert waar nodig de Datalekken Commissie.

In samenspraak met de FG formuleert de Zorgmanager Informatieveiligheid een opdracht voor de Datalekken Commissie. De leden van de Datalekken Commissie worden door de Zorgmanager Informatieveiligheid hierover vervolgens schriftelijk geïnformeerd, inclusief de termijn waarbinnen de RvB de rapportage wil ontvangen. Ook bijlage 3 'Informatie voor leden van de Datalekken Commissie', bijlage 4 'Informatie voor te interviewen interne personen door de Datalekken Commissie' en bijlage 5 'Informatie voor te interviewen (medewerkers van) derden door de Datalekken Commissie' worden door de Zorgmanager Informatieveiligheid aan de commissie ter beschikking gesteld.

5 *Startbijeenkomst Datalekken Commissie*

De Zorgmanager Informatieveiligheid plant een startbijeenkomst ter bespreking van de opdracht aan de Datalekken Commissie. Deze startbijeenkomst vindt in geval van een datalek plaats binnen één week na de melding van het datalek aan de AP.

De Zorgmanager Informatieveiligheid draagt zorg voor openstelling van alle beschikbare informatie inzake het datalek voor de leden van de Datalekken Commissie.

6 *Het datalekonderzoek*

De Datalekken Commissie stelt binnen de gestelde termijn en opdrachtverlening een (systematisch) (intern) onderzoek in naar de feitelijke toedracht van het (moge-

4 Te vinden op https://autoriteitpersoonsgegevens.nl onder 'melden'.

lijke) datalek. Binnen vier weken na de startbijeenkomst moet het onderzoek zijn afgerond. Daarbij onderzoekt de commissie ook of, en zo ja, hoe dergelijke incidenten in de toekomst kunnen worden voorkomen (het vermijdbaarheidsaspect).

De Datalekken Commissie is bevoegd om met iedereen te spreken, alle relevante documenten in te zien en toegang te hebben tot alle plaatsen. Dit alles in het kader van wat de commissie nodig acht ten behoeve van een zorgvuldige analyse. In relatie tot de externe bewerker gelden de afspraken zoals vastgelegd in de bewerkersovereenkomst. De commissie kan in overleg met, of op instigatie van de RvB besluiten om externe deskundigen te betrekken bij het onderzoek.

De Datalekken Commissie analyseert alle gegevens conform bijlage 6 'Format rapportage Datalekken Commissie' en bijlage 2 'Meldplicht datalekken in de Wet bescherming persoonsgegevens' van de AP. Vervolgens stuurt de commissie het conceptrapport ter verdere bespreking aan de Zorgmanager Informatieveiligheid en aan de FG. De Zorgmanager Informatieveiligheid organiseert, voordat de slotbijeenkomst plaatsvindt, een overleg met de leden van de Datalekken Commissie en de FG ter voorbespreking van het conceptrapport. De Datalekken Commissie legt het conceptrapport ter correctie op feitelijke onjuistheden voor aan de interne en externe geïnterviewden. Vervolgens stelt de Datalekken Commissie het rapport vast.

7 *Beoordeling of datalek gemeld dient te worden aan betrokkene(n)*

Is een datalek gemeld aan de AP, dan dient tevens vastgesteld te worden of het datalek ook moeten worden gemeld aan degenen om wier gegevens het gaat: de betrokkene(n). Of dit het geval is, is ter beoordeling van en advisering door de Datalekken Commissie. De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen kan tot stand komen met behulp van de schema's die zijn te vinden in de beleidsregels van de AP.

Indien het ETZ passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven (artikel 34a lid 6 Wbp). Bij twijfel hierover dient het datalek wel gemeld te worden aan de betrokkene(n).

Het datalek moet aan de betrokkene(n) worden gemeld, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a lid 2 Wbp). Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn. Bij dit laatste moet bijvoorbeeld gedacht worden aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen.

De melding aan de betrokkene(n) mag achterwege blijven als daarvoor zwaarwegende redenen aanwezig zijn (artikel 43 Wbp). Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit *noodzakelijk* is met het oog op de belangen die worden genoemd in dit artikel. Op grond van artikel 43 onderdeel e Wbp mag van de melding aan de betrokkene worden afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkene of van de rechten en vrijheden van anderen. De AP schetst in haar beleidsregels het volgende voorbeeld waarin een melding aan een betrokkene achterwege mag worden gelaten op basis van deze uitzondering:

'Er zijn gegevens gelekt over medische en psychosociale hulpvragen die kinderen buiten medeweten van hun ouders hebben gedaan. De verantwoordelijke meldt het datalek aan de Autoriteit Persoonsgegevens, en beroept zich op artikel 43, onder e, Wbp om de melding aan de betrokkenen achterwege te kunnen laten. Reden is dat de ouders door de melding op de hoogte zouden kunnen raken van de hulpvraag.'[5]

8 *Slotbijeenkomst in geval van een datalek: bespreking rapport en vaststellen verbetermaatregelen*

De RvB plant een slotbijeenkomst ter bespreking van het rapport van de Datalekken Commissie. Voor de slotbijeenkomst worden uitgenodigd de RvB, de leden van de Datalekken Commissie, het integraal management of daarmee gelijkgestelde manager en/of Manager ICT en/of Manager P&O en/of manager Facilitair bedrijf, de Zorgmanager Informatieveiligheid, de FG, de ISO, de communicatieadviseur en de juridisch adviseur. De genodigden ontvangen van de Zorgmanager Informatieveiligheid een afschrift van het conceptrapport. De RvB bespreekt tijdens de slotbijeenkomst het rapport en de voorgestelde SMART geformuleerde verbetermaatregelen. Tijdens de bijeenkomst wordt het standpunt van de RvB over het rapport van de Datalekken Commissie vastgesteld en worden afspraken over verbetermaatregelen vastgelegd. Tijdens de bijeenkomst wordt ook vastgesteld of en hoe het datalek aan de betrokkene(n) wordt gemeld. Na de bijeenkomst ontvangen de genodigden het definitieve rapport.

9 *Rapporteren aan de betrokkene(n)*

In opdracht van de RvB stelt de FG, in samenspraak met de communicatieadviseur en de juridisch adviseur, een kennisgeving aan betrokkene(n) op. De Zorgmanager Informatieveiligheid bepaalt in overleg met de FG wat aan de betrokkene(n) wordt gemeld. De melding bevat

5 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, p. 42.

in ieder geval de aard van het datalek, contactgegevens van het ETZ-informatiepunt waar de betrokkene(n) meer informatie over het datalek kan/kunnen krijgen, en de maatregelen die het ETZ de betrokkene(n) aanbeveelt om zelf te nemen om de negatieve gevolgen van de inbreuk te beperken. De betrokkene(n) wordt/worden individueel geïnformeerd.

Het datalek moet onverwijld gemeld worden aan de betrokkene(n). Dit houdt in dat het ETZ, na de ontdekking van het datalek, enige tijd mag nemen voor nader onderzoek zodat het ETZ de betrokkene op een behoorlijke en zorgvuldige manier kan informeren. Wel dient er hierbij rekening mee gehouden te worden dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder het ETZ de betrokkene(n) daarover informeert, hoe eerder deze in actie kan/kunnen komen.

In de melding aan de AP is al aangegeven of het ETZ het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer het ETZ dat gaat doen. De termijn die het ETZ in de melding aan de AP aangeeft, moet het ETZ ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat het ETZ dit aan de AP weten door middel van een aanpassing van de melding.

10 *Implementeren verbetermaatregelen*

De manager in wiens domein de verbetermaatregelen liggen is ervoor verantwoordelijk dat de door de Commissie Datalekken vastgestelde verbetermaatregelen worden geïmplementeerd. Deze manager ziet ook toe op de communicatie rondom en de uitvoering van die verbetermaatregelen. Ook zorgt hij ervoor dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering, en rapporteert hij over de voortgang aan de RvB. Indien bij een bewerker verbetermaatregelen nodig zijn, is de manager die opdrachtgever is van deze bewerker daartoe verantwoordelijk. De Zorgmanager Informatieveiligheid bewaakt de voortgang, onder eindverantwoordelijkheid van de RvB.

11 *Sluiten melding en vastlegging*

De Zorgmanager Informatieveiligheid informeert het lid van de raad van bestuur, de portefeuillehouder Informatieveiligheid, het betrokken integraal management, de betrokken organisatorisch manager, de direct bij de calamiteit betrokkenen (genodigden raad van bestuur), de Zorgmanager Informatieveiligheid, en/of Manager ICT en/of Manager P&O en/of manager Facilitair bedrijf, de FG, de ISO, de communicatieadviseur, en (indien van toepassing) de juridisch adviseur op het moment dat het datalek definitief afgehandeld is en de melding is gesloten. Vervolgens wordt de Datalekken Commissie door de RvB ontbonden. De leden van de Datalekken Commissie vernietigen de eventueel nog in hun bezit zijnde documentatie. Het 'datalekdossier' wordt digitaal bij de FG en het secretariaat van de Zorgmanager Informatieveiligheid gearchiveerd voor de duur van minimaal een jaar. Er kunnen redenen zijn om gedurende langere tijd te archiveren. Bijvoorbeeld minimaal drie jaar als de getroffen technische beschermingsmaatregelen voldoende bescherming hebben geboden om melding aan de betrokkene achterwege te kunnen laten, of als er zwaarwegende redenen aanwezig waren om de melding aan de betrokkene achterwege te laten.[6] De richtlijn zoals beschreven in bijlage 2 'Meldplicht datalekken in de Wet bescherming persoonsgegevens; beleidsregels' zal worden gehanteerd.

Tot slot

Deze procedure wordt gehanteerd bij het melden en afhandelen van (mogelijke) datalekken in het ETZ, dan wel van (mogelijke) datalekken die buiten het ETZ hebben plaatsgevonden, doch waarvoor het ETZ als verantwoordelijke wel de eindverantwoordelijkheid draagt (bijvoorbeeld bij een bewerker). Daarom is het ook van belang dat in een bewerkersovereenkomst duidelijke afspraken zijn of worden gemaakt over hoe te handelen bij een datalek. Samen met de Regionale Privacy Commissie voor de Gezondheidszorg (RPCG) heeft de Nederlandse Vereniging van Ziekenhuizen (NVZ) in november 2015 een standaardbewerkersovereenkomst vastgesteld waarin ook aandacht wordt besteed aan de meldplicht datalekken. Deze standaardbewerkersovereenkomst is beschikbaar op www.privacyindezorg.nl (Dossier Informatiebeveiliging).

6 Zie de beleidsregels van de AP, p. 46.