*Mr. C.M.M. Zwinkels**

De meldplicht datalekken: de bewerkersovereenkomst

49

Trefwoorden:
vestiging verantwoordelijke, bewerker, meldplicht datalekken, doorgifte derde-landen, Beleidsregels Autoriteit Persoonsgegevens, CBP Richtsnoeren beveiliging van persoonsgegevens 2013

1 De achtergrond

De Autoriteit Persoonsgegevens (AP) heeft beleidsregels opgesteld voor het toepassen van artikel 34a Wet bescherming persoonsgegevens (Wbp). Zij verlangt in de beleidsregels van de verantwoordelijken en hun bewerkers dat zij onderling met elkaar over een aantal onderwerpen afspraken gaan maken.[1] De reden is dat het nieuwe artikel 34a Wbp geen nadere voorschriften bevat over hoe de verantwoordelijke en de bewerker met elkaar moeten omgaan met betrekking tot een datalek. Artikel 14 Wbp is wel gewijzigd. De zorgplicht van de verantwoordelijke is in artikel 14 lid 3 sub c Wbp uitgebreid. Hij moet erop toezien dat zijn bewerker de verplichtingen nakomt die op de verantwoordelijke rusten met betrekking tot het doen van een melding over een inbreuk op de beveiliging, bedoeld in artikel 13 Wbp.

De verantwoordelijke is op grond van het aangepaste artikel14 Wbp belast met het melden van de datalekken, die binnenkomen bij zijn bewerker.[2] Omgekeerd moet de ICT-dienstverlener in de rol van bewerker zich ook actief gaan opstellen naar zijn verantwoordelijke.[3] Daarbij speelt dat de AP ervan uitgaat dat mogelijke beveiligingsincidenten juist bij de bewerker zullen binnenkomen. Daarom vraagt de autoriteit aandacht voor de volgende onderwerpen binnen de bewerkersovereenkomst.[4] De verantwoordelijke zal met zijn bewerker moeten vastleggen dat hij door laatstgenoemde geïnformeerd zal worden over nieuwe datalekken, inclusief de tijdigheid daarvan plus de beschikbaarheid van alle benodigde gegevens. En omdat de behandeling van een datalek een continuproces is gedurende dagen of zelfs weken, is het van groot belang dat de bewerker zijn verantwoordelijke op de hoogte stelt van niet alleen achteraf getroffen beveiligingsmaatregelen, maar ook vooraf in kennis stelt van nieuw op te stellen maatregelen.

Een derde onderwerp voor nadere vastlegging is of slechts de verantwoordelijke of ook de bewerker een melding aan de AP kan doen.

De kernvraag in dit artikel is wat de betekenis van de bewerkersovereenkomst is met het oog op het afhandelen van een datalek conform de normen opgenomen in artikel 34a Wbp. Deze vraag naar compliancy leidt tot de volgende subvragen:

- In hoeverre kun je met contractsbepalingen in de bewerkersovereenkomst de aansprakelijkheid van verantwoordelijke en bewerker op basis van de leer van de toerekenbare tekortkomingen inhoud geven? Zie paragraaf 2.
- Wat is de betekenis van de bijlagen bij de bewerkersovereenkomst? Dit, ervan uitgaande dat in de bijlagen afspraken zijn opgenomen over de uitvoering van de wettelijke meldplicht datalekken. Zie paragraaf 3.

In mijn opvatting is het succesvol nakomen van de wettelijke verplichting (de meldplicht datalekken) in sterke mate afhankelijk van het gaan werken met een van tevoren bedacht proces Meldplicht datalekken door de verantwoordelijke in overleg met zijn bewerker.[5] Bestudering van de beleidsregels van de AP leert dat de opgenomen en geïllustreerde vraagstructuren niet het karakter van procesactiviteiten binnen een organisatie en tussen organisaties hebben. Tevens ontbreekt in de beleidsregels de uitwerking van een aantal onderwerpen. Een voorbeeld is hoe partijen moeten communiceren naar indivi-

---

* **Cees Zwinkels MPC is jurist, Grotius Opleiding Informaticarecht, controller en werkt in opdracht van overheden en bedrijven aan vraagstukken op de terreinen van de privacybescherming, informatiebeveiliging, contracten en basis- en kernregistraties.**

1 Het begrip verantwoordelijke is gedefinieerd in artikel 1 sub d Wbp. De verantwoordelijke stelt het doel van en de middelen voor de verwerking van persoonsgegevens vast. De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. Zie artikel 1 sub e Wbp. Verantwoordelijke en bewerker sluiten samen een overeenkomst af met betrekking tot de verwerking van persoonsgegevens. De zogeheten bewerkersovereenkomst heeft haar juridische grondslag in artikel 14 Wbp.

2 *Kamerstukken II* 2012/13, 33662, 3, p. 16.

3 *Beleidsregels voor toepassing van artikel 34a van de Wbp*, AP 2015, p. 16.

4 *Beleidsregels voor toepassing van artikel 34a van de Wbp*, AP 2015, p. 14-15. In de voorafgaande Richtsnoeren beveiliging van persoonsgegevens 2013 van de AP zijn nadere regels opgenomen over de inrichting en de nakoming van de bewerkersovereenkomsten.

5 Zie bijvoorbeeld H. Candel & S. Nouwt, 'Help een datalek, een procedure voor het omgaan met datalekken', *P&I* 2016, afl. 3, p. 9 e.v.

duele en groepen van betrokkenen.[6] Dit geldt ook voor beantwoording van de vraag op welke wijzen de verantwoordelijke documenten met betrekking tot een datalek moet registreren en bewaren. Hierbij hef ik niet de beschuldigende vinger naar de AP. Nee, het gaat om onderwerpen, welke niet de AP, maar de verantwoordelijke en de bewerker zelf moeten organiseren binnen hun reguliere bedrijfsvoering.

2 De overeenkomst ex artikel 14 Wbp: toerekenbare tekortkomingen

Een standaardbepaling in een model-bewerkersovereenkomst is dat indien een van de partijen tekortschiet in de nakoming van zijn verplichtingen onder de Wbp de wettelijke aansprakelijkheidsregels van toepassing zijn. Deze regels zullen dus houvast moeten bieden in diverse complexe situaties, waarin verantwoordelijke en bewerker kunnen geraken. Wie draagt de gevolgen van een datalek, indien niet onmiddellijk na ontdekking adequate technische maatregelen zijn getroffen? Wie draagt de schade, als de doorlooptermijn van 72 uur ruimschoots wordt overschreden?[7] En wie draagt de gevolgen van het risico, als de betrokkenen te laat of onvoldoende worden geïnformeerd? En wie betaalt de extra kosten, indien de AP alsnog een bindende aanwijzing geeft, omdat artikel 34a lid 6 Wbp (geen melding aan betrokkenen) niet juist blijkt te zijn toegepast? En wie van de contractspartijen draait vervolgens op voor de door de AP opgelegde boete?

De praktijk leert dat het uitermate moeilijk is om in de bewerkersovereenkomst toerekenbare tekortkomingen te formuleren met het oog op de toepassing van artikel 6:74 BW, als het gaat om het voldoen aan de wettelijke meldplicht datalekken. Allereerst laten tekortkomingen in de betekenis van niet gehaalde resultaten zich in de bewerkersovereenkomst moeilijk definiëren. Een voorbeeld ter illustratie. De AP legt de 72-uurstermijn op aan de verantwoordelijke. Binnen deze termijn moet de melding aan de AP plaatsvinden. De termijn gaat lopen vanaf het moment van ontdekking van het datalek. Wanneer is er nu sprake van een tekortkoming? Als het slechts gaat om de technische constatering van een datalek, dan gaat de termijn lopen vanaf de constatering dat er een complex beveiligingsincident is opgetreden. Als er echter een juridische beoordeling nodig is om vast te stellen dat er een datalek is conform artikel 34a lid 1 Wbp, vangt de termijn aan vanaf het moment van het afronden van de beoordeling. Het antwoord op de vraag is niet helder in de beleidsregels van de AP.

En als het al zou lukken om tekortkomingen te definiëren, dan is er de tweede barrière. De beoordeling van de toerekenbaarheid van de tekortkoming is zeer complex. Dit, omdat de verantwoordelijke en zijn bewerker in hoog tempo, samen en tegelijkertijd de afhandeling van een datalek beïnvloeden.

De opvatting dat een bewerkersovereenkomst het karakter van een resultaatsverbintenis moet hebben, uitmondend in een service level agreement tussen partijen, deel ik niet. Het is niet haalbaar om resultaten in de betekenis van op te leveren producten of diensten plus performance te definiëren. De aanpak moet in mijn opvatting zijn dat verantwoordelijke en bewerker zich voortdurend bewust zijn van het vervullen van hun zorgplichten. De bewerker heeft een waarschuwingsplicht en informatieplicht. Deze twee zorgplichten hebben niet alleen een grondslag gekregen in de aankomende Verordening gegevensbescherming, maar ook in de jurisprudentie.[8] Ik zou een lans willen breken voor de opvatting dat in het verlengde van de twee genoemde zorgplichten verantwoordelijke en bewerker een controlplicht naar elkaar toe hebben.[9] Deze controlplicht is gerelateerd aan het proces Meldplicht datalekken. De essentie van de controlplicht is dat verantwoordelijke en bewerker tijdens de afhandeling van een datalek elkaar moeten aanspreken ten behoeve van het behalen van de procesresultaten op basis van het ontworpen en ingerichte proces Meldplicht datalekken.

De constatering is in deze paragraaf dat het geen aanbeveling verdient in het contract te preciseren wat de toerekenbare tekortkomingen zijn, maar in een bijlage te beschrijven welke procesresultaten door verantwoordelijke en/of bewerker behaald moeten worden. Deze opvatting sluit ook aan op de jurisprudentie, die zichtbaar wordt bij de behandeling van de geschillen over de uitvoering van ICT-contracten. In de situatie dat partijen kiezen voor een globaal contract zullen de gegevens over de werkwijzen tussen partijen in relatie met de risico's aanvullend vastgelegd moeten zijn, zodat de rechter zich een oordeel kan vormen over de vraag in hoeverre opdrachtgever en/of opdrachtnemer toerekenbare fouten hebben gemaakt. Een voorbeeld is de zaak van het *Jeroen Bosch Ziekenhuis versus Alert Life Sciences Computing*. Het hof kiest voor het uitgangspunt van een redelijke en billijke uitleg van de raamovereenkomst en de van het Addendum deel uitmakende bijlagen.[10]

3 De bijlagen

De stellingname in paragraaf 2 is dat het formuleren van toerekenbare tekortkomingen in de bewerkersovereenkomst geen aanbeveling verdient. Het maken van afspraken, vastgelegd in de bijlagen, leidt echter wel tot contractuele verplichtingen voor partijen. Immers, de bewerkersovereenkomst verwijst naar de bijlagen.

---

6 De betrokkene is degene op wie een persoonsgegeven betrekking heeft. Zie artikel 1 sub f Wbp.

7 De 72-uurstermijn geldt in de situatie van melding aan de AP, en niet bij melding aan betrokkenen. *Beleidsregels voor toepassing van artikel 34a van de Wbp*, AP 2015, p. 29.

8 Artikel 31 en 32 Verordening gegevensbescherming (COM(2012)11 def.; 012/0011). Hof Den Haag 8 maart 1984, *Computerrecht* 1984, p. 29-31 (*RBC/Brinkers*). Zie ook J.J. Krikke, 'Geen schending zorgplicht door software-onderhoudspartner', *Computerrecht* 2014/40.

9 Zie C. Stuurman, 'De aansprakelijkheid van de automatiseringsadviseur', *Computerrecht* 1986, p. 146-152.

10 Hof Den Bosch 17 februari 2015, ECLI:NL:GHSHE:2015:480, r.o. 3.7.3. Zie ook Rb. Den Haag 24 december 2014, ECLI:NL:RBDHA:2014:16568.

Onderwerpen voor de bijlagen zijn het platform van de risicoanalyse, standaarden en beveiligingsmaatregelen (bijlage 1), de procesdoeleinden en de procesactiviteiten meldplicht datalekken (bijlage 2) en de control (bijlage 3).

3.1 *Bijlage 1: Het platform van de risicoanalyse, standaarden en beveiligingsmaatregelen*

De redenering van het niet meer bestaande College bescherming persoonsgegevens (de voorloper van de AP) is dat er een risicoanalyse beschikbaar moet zijn als basis voor de te treffen beveiligingsmaatregelen.[11] Deze organisatiebrede risicoanalyse geeft naar mijn mening inzicht in de categorieën van potentiële datalekken bij de verantwoordelijke en zijn bewerker. Stel dat een overheidsdienst zijn ICT voor 100% heeft uitbesteed aan een cloudprovider binnen de EU. De omschrijving van potentiële datalekken in de risicoanalyse omvat het kunnen zoekraken van grote hoeveelheden data bij de subbewerkers van de cloudprovider.[12] Of ga uit van de situatie dat een bedrijf zijn klanten middels LinkedIn en Facebook toegang geeft tot databases in zijn backoffices. De typering van potentiële datalekken gaat uit van inbraken via de sociale media in de klantbestanden. Een derde voorbeeld van potentiële datalekken is de organisatiecultuur bij verantwoordelijke en/of bewerker waarin iedereen ongebreideld kan beschikken over alle bedrijfsdata.

Veronderstel dat de ISO-NEN-normen 27001 en 27002 gehanteerd worden in genoemde voorbeelden van potentiële datalekken. Er zal dan aandacht moeten zijn voor minimaal twee typen maatregelen, namelijk toegangsbeveiliging en beveiliging van het berichtenverkeer tussen de databases in het frontoffice en de backoffices.

De combinatie van inzichten vooraf in de potentiële datalekken, de gekozen standaarden en de getroffen maatregelen is een solide platform met behulp waarvan de ingeschakelde IB-specialisten en juristen bij de verantwoordelijke een binnengekomen potentieel datalek effectief en efficiënt kunnen onderzoeken.[13] Tegen de achtergrond van de inzichten is de verwachting dat er minder omvangrijk onderzoek voor het specifieke datalek nodig zal zijn om te beoordelen in hoeverre wordt voldaan aan de normen, opgenomen in artikel 34a lid 1 Wbp (melding aan de AP), artikel 34a lid 2 Wbp (melding aan betrokkene) en artikel 34a lid 6 Wbp (afzien van melding aan betrokkene). Een tweede voordeel is dat de AP de mogelijkheid krijgt om te beoordelen in hoeverre de verantwoordelijke zich reeds professioneel heeft voorbereid op het kunnen afhandelen van een specifiek datalek. Dit, op basis van de reeds beschikbare bedrijfsgegevens over mogelijke datalekken plus getroffen beveiligingsmaatregelen.

3.2 *Bijlage 2: Procesdoelstellingen en procesactiviteiten meldplicht datalekken*

A *De aanpak*

Het platform, beschreven in paragraaf 3.1, is de omgeving waarin de verantwoordelijke opereert. Dit ontslaat hem niet van de verplichting om zijn procesdoelstellingen en procesactiviteiten, gerelateerd aan de meldplicht datalekken, te omschrijven en toegankelijk te maken voor de interne afdelingen, zijn bewerker en indien nodig de AP.

A1 *Risicoanalyse als opstap naar de procesdoelstellingen*

De formulering van artikel 34a Wbp, aangevuld met de beleidsregels van de AP, geeft een eerste inzicht in de typen risico's bij de behandeling van een potentieel datalek. Om deze risico's beheersbaar te maken tijdens de afhandeling van een datalek is een proces Meldplicht datalekken nodig. De te formuleren procesdoeleinden moeten het antwoord zijn op het beheersen van de geïnventariseerde risico's.

De risico's en procesdoelstellingen worden nader geconcretiseerd onder A3.

A2 *Van procesdoelstellingen naar procesactiviteiten plus betrokken afdelingen*

De procesdoelstellingen kunnen slechts worden gerealiseerd met behulp van goed geoliede procesactiviteiten. Ik kies op basis van de beleidsregels van de AP voor een proces Meldplicht datalekken met de volgende procesactiviteiten:

- het datalek komt binnen (= procesactiviteit 1);
- de eerste (technische) maatregelen worden asap getroffen (= procesactiviteit 2);
- na binnenkomst vindt onderzoek naar het datalek plaats (= procesactiviteit 3);
- het besluit op basis van het onderzoeksresultaat is wel of juist niet te melden aan de AP (procesactiviteit 4.1), en wel of niet aan de betrokkenen (= procesactiviteit 4.2);
- de melding aan de AP vindt plaats (= procesactiviteit 5);
- de melding aan betrokkenen vindt plaats (= procesactiviteit 6);
- het datalekdossier wordt ingericht, bijgewerkt en bewaard (= procesactiviteit 7);
- de onderzoeken en besluiten zijn regelmatig onderwerp van auditing (= procesactiviteit 8);
- de auditresultaten ondersteunen mogelijke structurele verbetermaatregelen (= procesactiviteit 9).

Uiteraard kunnen de volgorde en zelfs de samenstelling van procesactiviteiten per meldplichtige organisatie anders toegesneden worden.

---

11 *Beveiliging van persoonsgegevens*, CBP februari 2013, p. 16.

12 Het begrip subbewerker is niet gedefinieerd in de Wbp. De bewerker (lees ICT-leverancier of -dienstverlener) kan zijn verplichtingen doorgeven aan subbewerkers, mits de verantwoordelijke daartoe in het contract met de bewerker de ruimte heeft geboden. *Kamerstukken II* 1997/98, 25892, 3, p. 63.

13 Zie ook W.F.R. Rinzema & F.B. Melis, 'Hoe kan de kwaliteit van ICT-systemen juridisch meetbaar worden gemaakt?', *Computerrecht* 2014/150.

Nadat de procesactiviteiten door de verantwoordelijke zijn geïnventariseerd zal deze de activiteiten toewijzen aan de interne afdelingen bij zichzelf en bij zijn bewerker. Betrokken ondersteunende afdelingen kunnen zijn Incidentenbeheer, Informatiebeveiliging, Juridische Zaken en Control.

A3 *Concretisering van de aanpak*

De geschetste aanpak van risico's inventariseren en de procesdoelstellingen formuleren (sub A1), en het toewijzen van de procesactiviteiten aan de betrokken afdelingen (sub A2) zal hieronder nader toegelicht worden binnen vier aandachtsgebieden: Termijnbewaking, Kwaliteit van het onderzoek, Dossieropbouw en Control.

B1 *Termijnbewaking*

Het risico is dat verantwoordelijke en bewerker er niet in slagen om de 72-uurstermijn te realiseren met het oog op het doen van een melding aan de AP.[14] De procesdoelstelling moet aangeven vanaf welk moment de termijn gaat lopen. Ik heb reeds in paragraaf 2 het onderwerp van de termijnbewaking aangeraakt. De keuze kan zijn de termijnbewaking te laten ingaan vanaf de technische constatering dat het om een aanzienlijk beveiligingsincident gaat. Het alternatief is dat de termijnmonitoring gaat lopen vanaf de constatering dat het gaat om een datalek conform artikel 34a lid 1Wbp.

Als de technische constatering uitgangspunt is, dan gaat de termijnbewaking in vanaf procesactiviteit 1 (het datalek komt binnen) tot en met procesactiviteit 5 (de melding aan de AP vindt plaats). Ervan uitgaande dat de termijn loopt vanaf procesactiviteit 1 zal de afdeling Incidentenbeheer of de afdeling Informatiebeveiliging belast zijn met de bewaking van de termijn.

In het alternatief 2, waarin de termijn gaat lopen vanaf het moment van vaststelling van een datalek op grond van artikel 34a lid 1 Wbp, is het juist om de afdeling Juridische Zaken aan te wijzen als de interne partij, die de 72-uurstermijn monitort.

In beide situaties zullen genoemde afdelingen de externe ICT-leverancier (lees de bewerker) op de hoogte moeten stellen van de hoeveelheid beschikbare uren binnen de doorlooptijd van de 72 uur ten behoeve van het kunnen verrichten van de toegewezen procesactiviteiten, zoals het verrichten van nader technisch onderzoek.

B2 *Kwaliteit van het onderzoek naar het datalek*

Het risico is dat achteraf niet meer geanalyseerd kan worden waarom een besluit tot melding wel of juist niet is genomen. De impact kan groot zijn. Er kan sprake zijn van een gebrekkig gemotiveerd besluit met als gevolg een bindende aanwijzing of zelfs een forse boete.[15] Dat kan uiteraard ook de situatie zijn ingeval de norm van 72 uur ruimschoots en zonder gegronde redenen wordt overschreden.

Procesdoelstelling moet zijn dat een besluit over het doen van een melding transparant en controleerbaar moet zijn. Hierbij horen procesactiviteit 3 (het doen van onderzoek) en procesactiviteit 4 (de melding aan de AP en aan de betrokkenen). Deze activiteit zal ondersteund moeten worden met interne formats. Allereerst is relevant dat de onderzoekers werken met een lijst met vragen voor het te verrichten feitenonderzoek. Welke typen feiten worden onderzocht en in hoeverre hebben deze betekenis voor de verwerking van persoonsgegevens? Daarnaast kunnen de beleidsregels van de AP de input zijn voor het opstellen van een vragenlijst, welke de onderzoekers kunnen afvinken met ja of nee, zodat duidelijk wordt in welke procesfase het onderzoek stopt:

- Is de Wbp wel van toepassing?
- Zo ja, is er sprake van een datalek?
- Zo ja, wordt voldaan aan het criterium in artikel 34a lid 1 Wbp?
- Zo ja, moet vervolgens getoetst worden aan artikel 34a lid 2 Wbp?
- Zo ja, kan op de vrijstellingsmogelijkheid in artikel 34a lid 6 Wbp een beroep worden gedaan?

De onderzoekers zullen werkzaam zijn bij de afdeling JZ en de afdeling IB. Het verdient aanbeveling in de procesomschrijving op te nemen dat de directie en de betrokken lijnmanager eindverantwoordelijk zijn voor het afwikkelen van het datalek.

B3 *Dossieropbouw*

De risico's zijn de volgende. Allereerst moeten de gegevens in het datalekdossier opgenomen worden die in de Wbp minimaal zijn genoemd.[16] Daarnaast kunnen de gegevens toegankelijk zijn voor onbevoegden. Ook kunnen documenten te lang of juist te kort bewaard worden.

Procesdoelstelling is dat de in de Wbp opgenomen dossiergegevens aanwezig zijn in het datalekdossier en in een beveiligde omgeving, en slechts toegankelijk zijn voor geautoriseerde medewerkers bij zowel de verantwoordelijke als zijn bewerker.

Zoals bekend opteert de AP voor bewaartermijnen van 1 jaar respectievelijk 3 jaar, echter zonder onderbouwde motivatie. Mij lijkt het uitgangspunt van artikel 10 Wbp nog steeds leidend. De verantwoordelijke bepaalt aan de hand van de concrete omstandigheden hoelang hij de verwerkte persoonsgegevens bewaart ten behoeve van de verwerkelijking van de achterliggende doelstelling. Bewaartermijnen kunnen afhankelijk van het datalek in relatie met de bedrijfsvoering bij de verantwoordelijke dus langer of zelfs korter dan de AP-termijnen zijn.

De procesactiviteit van het bewaren en het verwijderen van gegevens in het datalekdossier wordt toevertrouwd aan de afdeling Archivering of Digitale opslag. De afde-

14 De performancenorm van 72 uur betreft alleen de meldingen aan de AP. Het begrip 'onverwijld' is voor meldingen aan betrokkenen niet geconcretiseerd. Zie *Beleidsregels voor toepassing van artikel 34a van de Wbp*, AP 2015, p. 32.

15 M. Jansen (Dirkzwager), 'Art. 66 Wbp: Boetebevoegdheid: De grenzen van de nieuwe boetebevoegdheid van de Autoriteit Persoonsgegevens', *P&I* 2015, afl. 6. Zie ook 'Boetebeleidsregels AP 2016', *Stcrt.* 2043.

16 Zie artikel 34a lid 8 Wbp in relatie met artikel 34a lid 3 Wbp en artikel 34a lid 4 Wbp. In de beleidsregels geeft de AP geen nadere uitleg over de dossieropbouw.

ling IB en de afdeling JZ zijn slechts de gebruikers van het proces. Daarnaast zijn zij verantwoordelijk voor de kwaliteit van het datalekdossier binnen procesactiviteit 7 (het datalekdossier inrichten, onderhouden en bewaren).

B4 *Control*

Het risico is dat de verantwoordelijke vergeet het pakket van reeds getroffen structurele beveiligingsmaatregelen achteraf bij te stellen op basis van de evaluatie van de onderzochte datalekken van het ondersteunende proces Meldplicht datalekken.

De AP heeft in haar Richtsnoeren beveiliging van persoonsgegevens aangegeven dat het sluitstuk van de uitgevoerde risicoanalyse plus getroffen beveiligingsmaatregelen is het evalueren van de beveiligingsmaatregelen plus het organiseren van verbetermaatregelen.[17] De af te leiden procesdoelstelling is dat de genomen besluiten over datalekken jaarlijks worden geëvalueerd. De bijbehorende procesactiviteit is het verrichten van audits (procesactiviteit 8) als opstap naar het mogelijk treffen van verbetermaatregelen, inclusief wijzigingen in het proces Meldplicht datalekken (procesactiviteit 9).

De verantwoordelijke neemt in de bewerkersovereenkomst op dat hij een onafhankelijke derde de afgewikkelde datalekken kan laten analyseren en daaraan consequenties kan verbinden indien nodig. De consequenties kunnen leiden tot schadevergoeding en/of opzegging van de overeenkomst.

De verantwoordelijke zal zich moeten afvragen wat een passende audit is in de bewerkersovereenkomst.[18] Het voormalige College bescherming persoonsgegevens geeft enige sturing door op te merken dat de zwaarte en frequentie van de audits afhankelijk zijn van de gesignaleerde kwetsbaarheid plus opvolging van maatregelen.[19]

De bevoegdheid tot auditen achteraf biedt geen soelaas indien bij de behandeling van een datalek tussentijds moet worden bijgestuurd. De verantwoordelijke doet er verstandig aan vast te leggen dat hij op elk moment na binnenkomst van een potentieel datalek alle relevante gegevens over een datalek onverwijld bij de ICT-leverancier kan inzien en opeisen. Omgekeerd bepleit ik dat de bewerker binnen zijn geheimhoudingsplicht bij de verantwoordelijke alle procesgegevens en documenten ter zake van het specifieke datalek ook onmiddellijk moet kunnen inzien.

De reden voor het informatierecht in twee richtingen is dat partijen naar mijn mening over en weer een zorgplicht hebben om elkaar op de hoogte te stellen en bij te staan bij het verrichten van onderzoek ten behoeve van de melding.

De bevoegdheid van auditen komt te liggen bij de afdeling Interne Control, die onafhankelijke derden kan inhuren voor evaluatie en nader onderzoek naar de datalekken.

C *Constateringen*

Op basis van de opmerkingen sub A en B doe ik de volgende constateringen. De te inventariseren risico's zijn de input voor de te beschrijven procesdoelstellingen. Het opknippen van het proces Meldplicht datalekken in procesactiviteiten beoogt de realisatie van de procesdoelstellingen te waarborgen.

Met het oog op het kunnen beoordelen of de betrokken afdelingen bij de verantwoordelijke en de bewerker in de situatie van een datalek achteraf hebben voldaan aan hun zorgplichten is het zaak de rollen met betrekking tot de uitvoering van het proces te definiëren. De aanbevelingen hierboven gedaan vat ik samen.

72-uurstermijn: Kies welke afdeling de bewaking vanaf welk aanvangstijdstip zal doen; de afdeling Incidentenbeheer, de afdeling Informatiebeveiliging, of de afdeling JZ. Verplicht de ICT-leverancier zijn gegevens beschikbaar te stellen, mee te werken aan onderzoeken en maatregelen te treffen op het traject van procesactiviteit 1 tot en met 4.

Kwaliteit van het onderzoek: Leg de eindverantwoordelijkheid neer bij directie en lijnmanagement van de verantwoordelijke. Maak de bewerker verantwoordelijk voor deelonderzoeken. En: Laat het onderzoek doen door gekwalificeerde medewerkers van de afdeling IB en de afdeling JZ.

Dossieropbouw: De afdeling Archivering of Digitale opslag is leading.

Control: Wijs de afdeling Interne Control aan als de bewaker van de structurele kwaliteit van de verbetermaatregelen, inclusief het proces.

Wellicht ten overvloede gezegd, bovengenoemde aanbevelingen zijn alleen uitvoerbaar als zowel de betrokken interne afdelingen bij de verantwoordelijke als bij de bewerker over het proces Meldplicht datalekken, inclusief de datalekdossiers, kunnen beschikken. En het argument van de functiescheiding leidt tot de opmerking dat niet één afdeling verantwoordelijk mag zijn voor meerdere procesactiviteiten in relatie met de procesdoelstellingen.

4 De bewerker buiten de EU

Het complexe vraagstuk van hoe om te gaan met de bewerker die buiten de EU persoonsgegevens verwerkt, behandel ik op de volgende beknopte wijze in dit artikel.

Artikel 4 Wbp bevat het voorschrift dat de Wbp van toepassing is, mits de verantwoordelijke zijn vestiging in Nederland heeft én de verwerking van de gegevens binnen het kader van de activiteiten van de vestiging plaatsvindt. Zo niet, dan is de vraag of de ICT-middelen voor de verwerking van de gegevens zich in Nederland bevinden.

Aanvullend op de toepassing van artikel 4 Wbp zijn er de doorgifteregels in artikel 76, 77 en 78 Wbp. Een optie

17 *Beveiliging van persoonsgegevens*, CBP februari 2013, p. 26. *Kamerstukken I* 1999/2000, 25892, 92c, p. 15.
18 C.M.M. Zwinkels, 'Artikel 13 Wbp: De zorgplicht en informatiebeveiliging', *P&I* 2014, afl. 3, p. 123-129.
19 *Onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V.*, CBP december 2014, p. 24-25.

is dat de verantwoordelijke in zijn relatie met een niet-EU-bewerker gebruikmaakt van de EU-modelcontracten.[20] Gevolg is dat de verantwoordelijke ook in geval van een datalek bij genoemde bewerker een beroep kan doen op de afspraken, gemaakt in de bijlagen bij de overeenkomst en hierboven toegelicht.

5 Conclusies

Het omschrijven van toerekenbare tekortkomingen in de bewerkersovereenkomst is niet de weg om de zorgplichten van verantwoordelijke en bewerker te activeren met het oog op het afhandelen van een datalek. De aanpak moet zijn dat contractspartijen met elkaar afspraken maken in de bijlagen bij de bewerkersovereenkomst.

De verantwoordelijke heeft de zorgplicht voor het afhandelen van datalekken. De bewerker heeft een informatie- en waarschuwingsplicht. Het is wenselijk dat zowel verantwoordelijke als bewerker voor een controlplicht kiezen. Zij spreken elkaar aan op het verrichten van de procesactiviteiten om de procesdoelstellingen te realiseren.

Bijlage 1 van de bewerkersovereenkomst omvat de organisatiebrede risicoanalyse, de standaarden voor beveiliging en de getroffen maatregelen. Daarmee is het platform gedefinieerd waarop partijen opereren bij binnenkomst van een datalek.

Bijlage 2 verschaft de inzichten in de risico's, de procesdoelstellingen, en de procesactiviteiten, gerelateerd aan de meldplicht datalekken. Om te voorkomen dat de procesactiviteiten van iedereen zijn, is het relevant de procesactiviteiten toe te wijzen aan de betrokken interne afdelingen bij zowel verantwoordelijke als bewerker.

De verantwoordelijke stuurt de procesactiviteiten aan binnen de aandachtsgebieden van de 72-uurstermijn, de kwaliteit van het onderzoek, de dossieropbouw en de control.

Omdat de bewerker medeverantwoordelijk is voor de procesresultaten is het een voorwaarde dat hij toegang heeft tot de datalekdossiers bij de verantwoordelijke.

20 *Kamerstukken II* 2012/13, 33662, 6, p. 13. De wetgever beschrijft het voorbeeld van de bewerker in Frankrijk.