FIRST LAWYERS
Advocaten

Frankenslag 137
2582 HH Den Haag
T. 070 306 00 33
E. info@firstlawyers.nl

MYOBI B.V.
t.a.v. de heer drs. A.J. Biesheuvel
Frankenslag 137
2582 HH Den Haag

Datum: donderdag 31 maart 2016

mr. dr. A.W. Duthler
T. 070 306 00 33
F. 070 392 22 76
E. a.w.duthler@firstlawyers.nl

Betreft: **Bijsluiter bij weerbare bewerkersovereenkomst**

Geachte heer Biesheuvel, beste André,

MYOBI B.V. (hierna MYOBI) biedt aan haar cliënten zogenaamde weerbare bewerkersovereenkomsten aan. Deze cliënten kunnen dan de rol hebben van verantwoordelijke of de rol van bewerker. Een weerbare bewerkersovereenkomst heeft onder meer tot doel om risico's van ketenaansprakelijkheid en kostenrisico's te beheersen. Dat kan alleen als ook andere partijen in de keten een dergelijke weerbare bewerkersovereenkomst afsluiten. Er kunnen zich situaties voordoen waarin partijen dat niet willen. U heeft mij gevraagd te beschrijven wat de risico's zijn als andere partijen in de keten of het netwerk zo'n overeenkomst niet sluiten en of en op welke wijze uw cliënten hen op deze risico's moeten wijzen.

Uw cliënten hebben juridisch gezien een informatie- en waarschuwingsplicht. Zij dienen hun cliënten, leveranciers en andere relaties te informeren over de risico's van het niet sluiten van een weerbare bewerkersovereenkomst en hun cliënten, leveranciers en andere relaties dienen dat op hun beurt weer ten aanzien van hun cliënten, leveranciers en andere relaties te doen. Dit biedt hen tevens de gelegenheid te motiveren waarom zij hun eigen aansprakelijkheidsrisico's ten opzichte van hun cliënten en partners geheel of gedeeltelijk uitsluiten. Indien cliënten, leveranciers en andere relaties om welke reden dan ook geen weerbare bewerkersovereenkomst willen afsluiten en zich dus niet willen aansluiten bij een *Trusted Third Party* (TTP) zoals MYOBI, zijn de aansprakelijkheidsrisico's en kostenrisico's voor alle partijen in de keten of het netwerk minder goed te beheersen. Daar hoort een ander risicoprofiel bij en een andere verdeling van aansprakelijkheid. Dat licht ik in de bijgesloten notitie, die ik bijsluiter heb genoemd, nader toe. Deze notitie komt in de plaats van de notitie d.d. 26 oktober 2015 die ik u eerder in uw hoedanigheid van directeur van Duthler Associates toezond.

FIRST LAWYERS
Advocaten

Frankenslag 137
2582 HH Den Haag
T. 070 306 00 33
E. info@firstlawyers.nl

In bijgesloten notitie beschrijf ik de mogelijkheden en beperkingen van de weerbare bewerkersovereenkomst. Ik betrek daarbij de alternatieven die u onderkent. Dat zijn:

- de bewerkersovereenkomst met een Privacy Seal met een *maturity level* vastgesteld op basis van een bestuurlijk gesprek of op basis van een *self assessment;*
- de bewerkersovereenkomst zonder een Privacy Seal of ook wel de eenzijdige bewerkersovereenkomst.

Ik heb dat op een wijze gedaan die u in staat stelt deze notitie zelfstandig te verstrekken aan uw cliënten, die deze op hun beurt ook weer kunnen verstrekken aan hun cliënten, leveranciers en andere relaties. Ik beveel u van harte aan hen te wijzen op het belang van het vastleggen van de keuze met de bijbehorende consequenties die hun cliënten, leveranciers en andere relaties maken.

Vanzelfsprekend licht ik deze notitie graag mondeling aan u toe.

Met vriendelijke groet,

mr. dr. A.W. Duthler
Advocaat

FIRST LAWYERS
Advocaten

Frankenslag 137
2582 HH Den Haag
T. 070 306 00 33
E. info@firstlawyers.nl

Bijsluiter bij de weerbare bewerkersovereenkomst

Overzicht van mogelijkheden en beperkingen

First Lawyers

Den Haag, maart 2016

FIRST LAWYERS
Advocaten

Frankenslag 137
2582 HH Den Haag
T. 070 306 00 33
E. info@firstlawyers.nl

INHOUD

1. Inleiding

1. De traditionele bewerkersovereenkomst heeft een eenzijdig karakter. De verantwoordelijke legt de bewerker verplichtingen op. De bewerker aanvaardt deze. De bewerkersovereenkomst zoals bedoeld in artikel 14 van de Wbp gaat uit van een traditionele situatie waarin sprake is van een overeenkomst tussen één verantwoordelijke en één bewerker. Dit komt niet meer overeen met de huidige situatie waarin sprake is van gegevensverwerkingen die plaatsvinden in ketens of netwerken waarbij het bovendien soms lastig te bepalen is wie verantwoordelijke en wie bewerker is.[1]

2. De Wet meldplicht datalekken alsook de aanstaande Algemene verordening gegevensbescherming (Avg) vraagt om een aangepaste bewerkersovereenkomst. MYOBI heeft deze vormgegeven in de zogenaamde weerbare bewerkersovereenkomst. Daarnaast onderkent zij twee alternatieven, waarvan de eerste op haar beurt twee varianten kent. Dit zijn:

- de bewerkersovereenkomst met een Privacy Seal en een maturity level vastgesteld op basis van een bestuurlijk gesprek (variant 1) of op basis van een self assessment (variant 2);
- de bewerkersovereenkomst zonder een Privacy Seal of ook wel de eenzijdige bewerkersovereenkomst.

In deze bijsluiter worden de mogelijkheden en beperkingen van de weerbare bewerkersovereenkomst en de twee alternatieven beschreven.

2. De weerbare bewerkersovereenkomst

3. De weerbare bewerkersovereenkomst is er op gericht om in een keten of een netwerk van gegevensverwerkingen eenzelfde niveau van gegevensbescherming te realiseren en afspraken te maken over de manier waarop ketenpartijen met elkaar omgaan. Uitgangspunt is dat de verantwoordelijke transparantie biedt over zijn gegevensverwerkingen en de betrokkenen daarover informeert. De gegevensverwerkingen heeft hij gedocumenteerd en vastgelegd in zijn privacyboekhouding. Hij is ook daardoor goed in staat om aan de meldplicht datalekken te voldoen en transparantie te bieden aan betrokkenen. Dit is een voorwaarde voor betrokkenen om hun rechten te effectueren.

4. Partijen bij de weerbare bewerkersovereenkomst hebben zich aangesloten bij MYOBI, een *Trusted Third Party* (TTP) en houden zich aan een door MYOBI van te voren bepaald niveau van gegevensbescherming. In de TTP policy is bepaald welk niveau van gegevensbescherming voor de gehele keten of het gehele netwerk geldt. Er wordt vanuit gegaan dat deze partijen beschikken over een

[1] Overigens was dat ook de reden voor de wetgever om met de Wet meldplicht datalekken artikel 14 van de Wbp aan te passen.

Privacy Seal en kennis hebben betrokken uit het FG register.

5. Partijen die zijn aangesloten bij MYOBI, krijgen met gebruikmaking van het SBC managementsysteem de beschikking over een eigen elektronisch dossier – Dossier Organisatie geheten - waartoe ze hun wederpartij toegang geven.[2] In dit Dossier Organisatie worden onweerlegbaar vastgelegd de weerbare bewerkersovereenkomst, de aansluitovereenkomst en eventuele andere contracten. Ook het proces van contracteren kan worden vastgelegd. Indien een partij dit wenst, is het mogelijk om met behulp van een sticky policy aan te geven wie zij toegang wil geven tot haar dossier. Ook is het mogelijk voor een partij om - gekoppeld aan haar eigen Dossier Organisatie – met behulp van haar eigen SBC managementsysteem haar gegevensverwerkingen te documenteren, de toegang die zij aan betrokkenen tot hun gegevens heeft gegeven onweerlegbaar vast te leggen of het onverwijld melden van incidenten inclusief de afhandeling daarvan vast te leggen. Deze laatste mogelijkheden maken niet standaard onderdeel uit van de weerbare bewerkersovereenkomst.

6. Het niveau van gegevensbescherming wordt bepaald door het gemeenschappelijk normenkader dat is afgeleid uit het policy framework privacy. TTP Associates beheert het gemeenschappelijk normenkader alsook het policy framework privacy.[3] Daarnaast kan MYOBI gevraagd worden de onderzoeken naar de oorzaken van beveiligingsincidenten te coördineren, kan MYOBI op verzoek de afhandeling van datalekken faciliteren en coördineren en kan MYOBI op verzoek de communicatie naar andere verantwoordelijken en (sub-)bewerkers, alsook indirect naar de AP en betrokkenen in geval van datalekken faciliteren. Faciliteren in die zin dat de functies en diensten van de TTP gebruikt kunnen worden en dat MYOBI de momenten en de inhoud van de communicatie onweerlegbaar vaststelt.

7. MYOBI heeft op grond van de TTP policy de bevoegdheid in te grijpen, boetes op te leggen of het lidmaatschap van MYOBI op te zeggen als een partij zich niet houdt aan de afspraken en de mores zoals vastgelegd in de weerbare bewerkersovereenkomst, de aansluitovereenkomst en TTP policy zelf. Ook kan zij een bemiddelende rol spelen in geval van geschillen tussen partners in de keten of het netwerk.

3. Mogelijkheden en beperkingen van een weerbare bewerkersovereenkomst

8. De weerbare bewerkersovereenkomst voorziet zoals gezegd in gemeenschappelijke afspraken over het niveau van gegevensbescherming, het niveau van beveiliging, de te treffen beveiligingsmaatregelen, de nadere invulling van het begrip ‘onverwijld’, de naleving van de meldplicht in geval van inbreuken op de beveiliging alsmede de afhandeling daarvan. Zo worden - via aansluiting bij MYOBI - gemeenschappelijke criteria ontwikkeld om te bepalen of er sprake is van een beveiligingsincident met

[2] Indien de wederpartij de weerbare bewerkersovereenkomst accepteert, krijgt ze vervolgens haar eigen dossier. Indien de wederpartij de weerbare bewerkersovereenkomst niet accepteert, blijft ze als verbonden partij in het dossier van de aanbiedende partij genoemd staan.
[3] TTP Associates is de ontwikkelings- en beheerorganisatie die onderdeel uitmaakt van Duthler Associates. Zie ook www.ttp.associates.

ernstige gevolgen voor de bescherming van persoonsgegevens of van een aanzienlijke kans op ernstige gevolgen voor de bescherming van persoonsgegevens. Er worden geen onnodige onderzoekskosten gemaakt in geval van inbreuken op de beveiliging en meldingen aan de toezichthouder en betrokkenen omdat de TTP policy bepaalt dat eventuele onderzoekskosten voor rekening zijn van die partij die het initiatief neemt of opdracht geeft tot het uitvoeren van onderzoeken.

9. De weerbare bewerkersovereenkomst voorziet niet alleen in gemeenschappelijke afspraken over de hierboven genoemde onderwerpen. De weerbare bewerkersovereenkomst voorziet ook in gemeenschappelijke afspraken – in de vorm van een gemeenschappelijke taal en mores - over het documenteren van verwerkingen (de privacyboekhouding), het voldoen aan de informatieplicht en het effectueren van rechten van betrokkenen, zoals het inzage- en correctierecht en het recht van verzet. Ook deze afspraken beheert MYOBI. Het voordeel hiervan is dat in combinatie met het Privacy Seal de verantwoordelijke en de bewerker in ruime mate invulling kunnen geven aan het beginsel van transparantie. Zij bieden transparantie over de verwerkingen die zij voeren en wie de functionaris gegevensbescherming is. Daarnaast kunnen de betrokkenen weten dat hun persoonsgegevens worden verwerkt en dat en op welk niveau de verantwoordelijke en bewerker de toepasselijke privacywetgeving naleven.

10. De weerbare bewerkersovereenkomst maakt het mogelijk aansprakelijkheidsrisico's evenwichtig te verdelen. Omdat de bij MYOBI aangesloten partijen van elkaar weten aan welk niveau van gegevensbescherming zij zich conformeren en MYOBI kan ingrijpen bij niet- naleving daarvan[4], zijn zij in staat om hun aansprakelijkheidsrisico's te beheersen en beperkt te aanvaarden.

11. In deze bewerkersovereenkomsten zijn tevens concrete veiligheidsnormen vastgelegd waaraan partijen zich conformeren. In geval van overtreding van deze veiligheidsnormen wordt voorshands aangenomen dat opgekomen schade causaal verband houdt met deze overtreding – tenzij het tegendeel wordt bewezen - en dus de overtreder aansprakelijk is. Dit verlicht eventuele discussies over bewijs en bewijslastverdeling.

12. Daarnaast bevat de weerbare bewerkersovereenkomst afspraken voor die situaties waarin de AP een boete oplegt aan een verantwoordelijke wegens het niet onverwijld melden van een datalek, terwijl dat te wijten is of toe te rekenen valt aan een bewerker of andere partner in de keten en de verantwoordelijke dus een grond heeft om deze te verhalen op de bewerker of die andere partner in de keten.

13. Omdat partijen zich houden aan een bepaald niveau van gegevensbescherming en dit via het Privacy Seal kenbaar maken, zijn zij duidelijk over de verwachtingen die zij wekken naar hun cliënten en partners. Ook dit vermindert de kansen dat zij aansprakelijk kunnen worden gesteld door cliënten,

[4] Middels het bestuurlijk overleg kan daarvan blijken of bij interne of externe controles. MYOBI kan in het uiterste geval de aansluitovereenkomst opzeggen en daarmee het lidmaatschap van MYOBI.

partners of andere derden die door hun vermeend handelen of nalaten schade hebben geleden.

14. Daarnaast biedt de kennis die via het FG-register beschikbaar wordt gesteld meer zekerheid dat de Wbp, die samen met andere privacywetgeving in het normenkader is uitgewerkt, kan worden nageleefd. Ook de afgesproken interne en externe controles dragen daar aan bij. Ook deze factoren verminderen de risico's op aansprakelijkheid.

15. Omdat MYOBI de-escalerend optreedt, voorkomt of dempt het conflicten met toezichthouders of met andere partijen in de keten of het netwerk. Zonder deze functie bestaat het risico dat partijen zelf onnodige kosten maken zoals die voor het inhuren van een advocaat, beveiligingsspecialisten en of IT auditors of met kosten geconfronteerd worden zoals die van imagoschade waarvan zij de vergoeding over en weer civielrechtelijk van elkaar zullen vorderen.

16. Tot slot bevat de weerbare bewerkersovereenkomst een geschillenregeling die bepaalt dat in geval van geschillen de oplossing daarvan eerst wordt beproefd via mediation. Dit bespaart aanzienlijke kosten die anders voor een gewone juridische procedure bij een overheidsrechter moeten worden gemaakt.

4. Mogelijkheden en beperkingen voor bestuurders en feitelijk leidinggevenden

17. MYOBI maakt gebruik van het zogenaamde SBC managementsysteem voor het vastleggen en ontsluiten van gegevens in elektronische dossiers van partijen. Deze elektronische dossiers kunnen behalve voor rechtspersonen ook voor natuurlijke personen worden aangemaakt en gebruikt.[5] In deze notitie ga ik uit van het gebruik door rechtspersonen of andere organisaties.[6] Ook bestuurders en feitelijk leidinggevenden kunnen echter in voorkomende gevallen persoonlijk boetes opgelegd krijgen. Dat is het geval als zij door de toezichthouder als 'medepleger' worden gekwalificeerd. Voor die gevallen is het nuttig dat deze bestuurders en feitelijk leidinggevenden hun eigen persoonlijk elektronisch dossier hebben dat gefaciliteerd wordt door MYOBI. Op die manier kunnen zij hun informatiepositie en daarmee hun bewijspositie veilig stellen en de risico's om als medepleger te worden beschouwd door de AP of het Openbaar Ministerie verminderen. In ieder geval zijn zij 'weerbaar' als zij in een bestuurlijk handhavingstraject of strafrechtelijk opsporingsonderzoek worden betrokken.

18. Ook in civielrechtelijke procedures kan een persoonlijk dossier voor bestuurders, commissarissen en feitelijk leidinggevenden en of beleidsbepalers uitkomst bieden. Dat is in het geval van onbehoorlijke taakvervulling, aansprakelijkheid wegens wanbeleid of een ingeval van een onrechtmatige daadsactie.

19. Op grond van artikel 2:9 BW is een bestuurder gehouden tot een behoorlijke vervulling van zijn taak. Elke bestuurder is voor het geheel aansprakelijk terzake van onbehoorlijk bestuur, tenzij hem geen

[5] Het dossier voor rechtspersonen en andere organisaties heet Dossier Organisatie. Het dossier voor natuurlijke personen heeft Dossier Personen.
[6] De rechtspersoon of andere organisatievorm sluit immers de bewerkersovereenkomst.

ernstig verwijt kan worden gemaakt en hij niet nalatig is geweest in het treffen van maatregelen om de gevolgen van onbehoorlijk bestuur af te wenden. Om van deze disculpatiemogelijkheid gebruik te kunnen maken biedt een persoonlijk dossier de bestuurder of feitelijke beleidsbepalers relevante verantwoordingsinformatie.

20. Op grond van artikel 2:248 BW of 2:138 BW kan een bestuurder of feitelijk beleidsbepaler hoofdelijk aansprakelijk worden gesteld indien het bestuur zijn taak kennelijk onbehoorlijk heeft vervuld en aannemelijk is dat dit een belangrijke oorzaak is van het faillissement. Indien het bestuur niet aan zijn plicht van artikel 2:10 BW (of 2:394 BW) heeft voldaan, dan wordt vermoed dat onbehoorlijke taakvervulling een belangrijke oorzaak is van het faillissement. Dit is een onweerlegbaar wettelijk vermoeden. Indien het bestuur niet op een zorgvuldige wijze aan de plicht van artikel 2:10 BW heeft voldaan dan is er sprake van een weerlegbaar wettelijk vermoeden. Artikel 2:10 betreft de plicht van de vermogenstoestand van de rechtspersoon en van alles betreffende de werkzaamheden van de rechtspersoon op zodanige wijze een administratie te voeren en de daartoe behorende boeken, bescheiden en andere gegevensdragers op zodanige wijze te bewaren dat te allen tijde de rechten en verplichtingen van de rechtspersoon kunnen worden gekend. Hierin kan met toepassing van artikel 2:391 lid 5 ook worden gelezen de verplichting een privacyboekhouding te voeren en ook voor het overige te voldoen aan de eisen van de Wet meldplicht datalekken. In lid 5 van artikel 2:391 wordt namelijk verwezen naar een algemene maatregel van bestuur waarin nadere voorschriften worden gesteld. Deze algemene maatregel van bestuur verwijst naar een governance code die voorschrijft dat – kort door de bocht - bestuurders en commissarissen in hun jaarverslag melding moeten maken van strategische, operationele, financiële, verslaggevings- en compliancerisico's. Zo nodig geven zij een in-controlstatement af dat de interne risicobeheersings- en controlesystemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat en dat de interne risicobeheersings- en controlesystemen naar behoren hebben gewerkt.

21. De corporate governance code waarnaar artikel 2:391 lid 5 BW is wettelijk verankerd en krijgt steeds meer het karakter van materiële wetgeving. Zo is in een uitspraak van de Hoge Raad bepaald dat de code mede inhoud geeft aan de eisen van redelijkheid en billijkheid naar welke volgens artikel 2:8 BW degenen die krachtens de wet of de statuten bij de vennootschap zijn betrokken zich jegens elkaar moeten gedragen en aan de eisen die voortvloeien uit een behoorlijke taakvervulling waartoe elke bestuurder ingevolge artikel 2:9 BW gehouden is.[7]

22. Dan is daar tot slot nog de onrechtmatige daadsactie op grond van artikel 6:162 BW jo artikel 2:9 BW. Op deze grond kan een bestuurder, commissaris of feitelijke beleidsbepaler aansprakelijk worden gesteld. Er moet dan sprake zijn van een onrechtmatige gedraging, schade en causaal verband tussen de onrechtmatige gedraging en de schade die is geleden. De onrechtmatige gedraging wordt nader ingekleurd door artikel 2:9 BW.

[7] HR 13 juli 2007, NJ 2007/434, m.nt.J.M.M. Maeijer (ABN AMRO).

5. Mogelijkheden en beperkingen van een bewerkersovereenkomst met Privacy Seal en FG kennis

23. De bewerkersovereenkomst met Privacy Seal bevat regelingen voor de verdeling van aansprakelijkheidsrisico's, te vergoeden schades zowel wat betreft hoogte als soort schade en de verdeling van bewijslast. Omdat deze regeling uitgaat van een bepaald niveau van gegevensbescherming, kennis over de toepassing en interpretatie van de Wbp aanwezig is en partijen ten opzichte van elkaar daarover transparant zijn, is het mogelijk de risico's enigszins evenwichtig te verdelen. Deze regeling kan echter alleen worden ingeroepen ten opzichte van de partij met wie de overeenkomst is afgesloten. Deze vorm van bewerkersovereenkomst biedt dus alleen de mogelijkheid om de aansprakelijkheidsrisico's te beperken en te beheersen ten opzichte van de partijen met wie de overeenkomst is gesloten. Niet ten opzichte van de partijen die geen weerbare bewerkersovereenkomst hebben afgesloten en dus geen lid zijn van MYOBI.

24. In deze bewerkersovereenkomsten zijn tevens concrete veiligheidsnormen vastgelegd waaraan partijen zich conformeren. In geval van overtreding van deze veiligheidsnormen wordt voorshands aangenomen dat opgekomen schade causaal verband houdt met deze overtreding – tenzij het tegendeel wordt bewezen - en dus de overtreder aansprakelijk is. Dit verlicht discussies over bewijs en bewijslastverdeling ten aanzien van de partijen met wie zij een contract hebben gesloten. Niet ten aanzien van andere partijen in de keten of in het netwerk.

25. In geval van een boete die wordt opgelegd aan de verantwoordelijke, terwijl deze wordt veroorzaakt door een gedraging van een partij in de keten, niet zijnde de bewerker waarmee de verantwoordelijke een overeenkomst heeft afgesloten is het lastig voor de verantwoordelijke om de schade die daardoor wordt veroorzaakt te verhalen bij de schadeveroorzakende partij. De verantwoordelijke heeft dan immers geen overeenkomst met deze partij waarin dit van te voren is bepaald, maar moet terugvallen op andere rechtsgronden dan de rechtsgrond van wanprestatie, bijvoorbeeld onrechtmatige daad of zaakwaarneming. Het is lastiger om een vordering op deze rechtsgronden toegewezen te krijgen. Bovendien is een rechtsgang vaak kostbaar en neemt veel tijd in beslag.

26. Omdat partijen zich houden aan een bepaald niveau van gegevensbescherming en dit via het Privacy Seal kenbaar maken, zijn zij duidelijk over de verwachtingen die zij wekken naar hun cliënten en partners. Ook dit vermindert de kansen dat zij aansprakelijk kunnen worden gesteld door cliënten, partners of andere derden die door hun vermeend handelen of nalaten schade hebben geleden.

27. In de 'gewone' bewerkersovereenkomst kunnen weliswaar afspraken worden opgenomen over de afhandeling van datalekken, maar deze afspraken gelden slechts tussen de verantwoordelijke of bewerker en hun klanten met wie deze bewerkersovereenkomst wordt afgesloten. De afspraken die de klanten van de verantwoordelijke of bewerker ofwel in hun hoedanigheid van verantwoordelijke ofwel in hun hoedanigheid van bewerker en of sub-bewerker weer met andere bewerkers of verantwoordelijken

sluiten, vallen hier buiten. Een bewerkersovereenkomst geldt immers slechts tussen de partijen die deze overeenkomst tekenen. Derden kunnen in beginsel geen rechten ontlenen aan deze overeenkomst, noch kunnen verplichtingen aan derden op basis van deze overeenkomst worden opgelegd. De mogelijkheid om kosten te beperken bij de afhandeling van datalekken is er niet of nauwelijks.

28. Daarnaast biedt deze bewerkersovereenkomst geen oplossing voor de noodzakelijke coördinatie van uitvoering van onderzoeken naar de oorzaken van beveiligingsincidenten. Indien deze onderzoeken niet worden gecoördineerd tussen verantwoordelijken, bewerkers en sub-bewerkers in de keten of het netwerk, kunnen de kosten daarvan behoorlijk de pan uit rijzen. Partijen zullen deze kosten willen kunnen afwentelen op de partij voor wiens risico en rekening deze onderzoeken uiteindelijk blijken te moeten komen. Als geen overeenkomst is gesloten tussen deze partijen, wordt dat een stuk lastiger.

29. Verantwoordelijken en bewerkers die kiezen voor deze bewerkersovereenkomst moeten daarnaast nog rekening houden met de kans dat hun klanten op verschillende wijzen invulling gaan geven aan het toezicht dat zij moeten houden op de feitelijke naleving door de bewerker van hun wettelijke verplichtingen. De vraag is hoe zij er voor kunnen zorgen dat de kosten van het – verschillend – uitoefenen van het toezicht door individuele klanten niet uit de hand lopen.

30. Uit het *maturity level* van het Privacy Seal kan worden afgeleid of alle verwerkingen zijn gedocumenteerd (de privacyboekhouding), of aan de informatieplicht wordt voldaan en of de rechten van betrokkenen kunnen worden geeffectueerd, zoals het inzage- en correctierecht en het recht van verzet. Hierover zijn geen gemeenschappelijke afspraken in de keten of het netwerk gemaakt en MYOBI kan niet ingrijpen in geval van niet-naleving ervan. Het voordeel van het Privacy Seal is dat de verantwoordelijke en de bewerker in zekere mate – afhankelijk ook van het *maturity level* - invulling kunnen geven aan het beginsel van transparantie. Zo kunnen zij transparantie bieden over de verwerkingen die zij voeren en wie de functionaris gegevensbescherming is. Zo kunnen de betrokkenen weten dat en op welke wijze hun persoonsgegevens worden verwerkt.

6. Mogelijkheden en beperkingen van een eenzijdige bewerkersovereenkomst

31. Indien een bewerker om welke reden dan ook geen weerbare bewerkersovereenkomst of gewone bewerkersovereenkomst met Privacy Seal wenst af te sluiten en zich dus ook niet aansluit bij MYOBI, dan is er goede grond voor de verantwoordelijke om de aansprakelijkheidsrisico's eenzijdig neer te leggen bij de bewerker.[8] De verantwoordelijke heeft immers weinig tot geen zekerheid dat de bewerker handelt in overeenstemming met de Wbp.

32. In deze bewerkersovereenkomsten zijn geen concrete veiligheidsnormen vastgelegd waaraan partijen zich conformeren. In geval van overtreding van de Wbp die schade tot gevolg heeft, kunnen uitvoerige

[8] Ditzelfde geldt omgekeerd indien de verantwoordelijke er niet voor kiest een weerbare bewerkersovereenkomst af te sluiten.

discussies ontstaan over de oorzaken van de schade en het causale verband tussen oorzaken en opgetreden schade, alsook over de bewijslastverdeling tussen partijen.

33. Onderzoekskosten in geval van datalekken alsook andere kosten die worden gemaakt voor de afhandeling er van en juridische kosten indien partijen aansprakelijk worden gesteld voor schade als gevolg van datalekken, zijn moeilijk te beperken.

34. Kosten van het uitvoeren van toezicht op de naleving van de bewerkersovereenkomst en de Wbp zijn moeilijk te beperken omdat van te voren geen niveau van gegevensbescherming is overeengekomen, en geen gemeenschappelijk normenkader waaraan partijen zich conformeren. De kosten hiervoor moeten voor elke overeenkomst opnieuw worden gemaakt. Daarmee is het toezicht zelf nog niet uitgevoerd.

35. De verantwoordelijke en bewerker bieden geen transparantie over de naleving van de privacywetgeving, noch over het niveau van gegevensbescherming. Betrokkenen en andere derden hebben geen zekerheid over de mate van compliance van de verantwoordelijke en bewerker.

7. Tot slot

36. Uitgangspunt is dat de belangen van cliënten van verantwoordelijken en bewerkers centraal staan. Vanzelfsprekend. De belangen van cliënten hebben geen absoluut karakter, maar worden begrensd door de verantwoordelijkheid die verantwoordelijken en bewerkers kunnen dragen voor de naleving van de Wbp, de Wet meldplicht datalekken en straks de Avg. De naleving van deze wet- en regelgeving door verantwoordelijken en bewerkers worden immers beïnvloed door de naleving door hun cliënten. We komen dan uit bij de beheersing van risico's op niet-naleving van de genoemde wetten. Die risico's moeten zo goed mogelijk worden beheerst.

37. De meeste mogelijkheden en minste beperkingen bieden de weerbare bewerkersovereenkomsten. Deze bieden een gemeenschappelijk normenkader, een gemeenschappelijk beschermingsniveau en verantwoordingsinformatie voor bestuurders, commissarissen, feitelijk leidinggevenden en feitelijke beleidsbepalers. Iedere bij MYOBI aangesloten partij is aanspreekbaar op de naleving van het gemeenschappelijke beschermingsniveau, verbindt zich tot het uitvoeren van interne en externe controles en in geval van incidenten of geschillen MYOBI te accepteren als de partij die mediation faciliteert. In geval van een claim of boete biedt de weerbare bewerkersovereenkomst de organisatie en haar bestuurders en feitelijk leidinggevenden een bewijspositie.

38. Niet alle contractspartijen van verantwoordelijken en bewerkers zullen bij voorbaat een weerbare bewerkersovereenkomst willen, en verantwoordelijken en bewerkers kunnen hen ook niet verplichten zich aan te sluiten bij MYOBI. In dat geval verdient het de voorkeur dat zo'n contractspartij in ieder geval over een Privacy Seal beschikt en gebruik maakt van de kennis van het FG-register. Op die manier is het niveau van gegevensbescherming helder en worden aansprakelijkheidsrisico's nog enigszins

beheerst. Als een cliënt ook dat niet ziet zitten, is het gerechtvaardigd de aansprakelijkheidsrisico's eenzijdig te beleggen. De aanbiedende partij (van de weerbare bewerkersovereenkomst) moet wel kunnen aantonen dat hij zijn wederpartij deze overeenkomst heeft aangeboden en hem geïnformeerd en gewaarschuwd hebben voor de voor- en nadelen alsmede de risico's die het niet aangaan van zo'n overeenkomst met zich meebrengen. Dat kan deze doen door het proces van contracteren in zijn Dossier Organisatie en eventueel in zijn Dossier Personen vast te leggen.

8. Overzicht

Hierna volgt een overzicht van de mogelijkheden en beperkingen van de weerbare bewerkersovereenkomst versus de eenzijdige bewerkersovereenkomst.

	Weerbare bewerkersovereenkomst	Niet-weerbare bewerkersovereenkomst
Aansprakelijkheid en schadevergoeding	Aansprakelijkheid evenwichtig verdeeld.	Aansprakelijkheid eenzijdig belegd.
	Schade als gevolg van opgelegde boete is ex TTP policy verhaalbaar op schadeveroorzakende partij.	Schade als gevolg van opgelegde boete is moeilijk verhaalbaar en brengt veel kosten met zich mee.
Bewijspositie	Goed, zowel in civiele, strafrechtelijke als administratieve procedures.	Onduidelijk, waarschijnlijk beperkt.
Onderzoekskosten	Onderzoek naar oorzaken incidenten kunnen gecoördineerd plaatsvinden.	Onderzoeken naar oorzaken incidenten vindt ongecoördineerd plaats en waarschijnlijk door meerdere partijen.
	Onderzoekskosten beperkt	Onderzoekskosten onbepaald
Juridische kosten	TTP policy voorziet in mediation. Deze is goedkoper en verloopt sneller dan een procedure bij de gewone rechter.	Om schade vergoed te krijgen is gang naar de rechter noodzakelijk.
Toezichtskosten	Toezichtskosten beperkt	Toezichtskosten onbepaald
Niveau van gegevensbescherming duidelijk	Partijen conformeren zich aan het door MYOBI vastgestelde niveau van gegevensbescherming. MYOBI kan differentiëren naar verschillende niveaus van beveiliging. Het Privacy Seal maakt dat mogelijk.	Partijen voldoen aan de wet. Er is geen mogelijkheid te differentiëren tussen verschillende niveaus van gegevensbescherming.
	Het Privacy Seal zorgt er voor dat het maturitylevel van een ketenpartij voor iedereen kenbaar is. De ketenpartij wekt gerechtvaardigde verwachtingen.	
Zekerheid over naleving	Kennis over toepassing, interpretatie en naleving privacywet is geborgd.	Kennis over toepassing, interpretatie en naleving privacywet is niet geborgd.
	Vanwege afgesproken controles meer zekerheid over naleving privacywet.	Minder zekerheid over naleving privacywet.

Overzicht: mogelijkheden en beperkingen van de weerbare bewerkersovereenkomst versus de eenzijdige bewerkersovereenkomst.