Policy

Versie: 1.5

Datum: 5 september 2017

www.ttp.associates

Inhoud

1. Inleiding 3
2. Waarom het Privacy Seal? 5
3. Wat is het Privacy Seal? 6
   3.1. Criteria op basis waarvan het Privacy Seal wordt verleend 6
   3.2. Niveaus van volwassenheid 6
   3.3. Afbakening: wat is het wel en wat is het niet? 9
   3.4. Geldigheidsduur 10
4. Wat heb ik aan het Privacy Seal? 11
5. Hoe kom ik aan het Privacy Seal? 12
   5.1. Werkwijze 12
   5.2. Verdeling taken en verantwoordelijkheden 14
   5.3. Criteria voor intrekking van het Privacy Seal 14
6. Hoe past het Privacy Seal bij de geldende en aanstaande privacywet- en regelgeving? 15
7. De rol van de FG 16
8. Relatie met het FG Register en het FG Cluster 17
9. Relatie met Trusted Third Party en TTP-policy 17
10. Relatie met het Legal Entity Framework (LEF) 18
11. Overige informatie en vragen 19

Bijlage: maturity levels 20

Versiebeheer

versie	Datum	naam	Opmerkingen
0.1	2014, 5 dec	AJB,PC	Initieel document
1.0	2015, 19 jan	PC	Criteria verduidelijkt
1.1	2015, 2 april	PC	Maturity scan toegevoegd
1.2	2015, 4 mei	PC	Maturity levels vervangen door vs 3.6
1.3	2015, 11 mei	PC	"TTP" en "policy framework" in bijlage, level 0 in 3.2
1.4	2016, 18 mrt	AWD,AJB	Geactualiseerd
1.5	2017, 5 sept	AWD,AJB	Geactualiseerd

1. Inleiding

Ontwikkelingen in de wet- en regelgeving rond gegevensbescherming leiden tot grotere aansprakelijkheidsrisico's dan tot nu toe het geval was. Rechten van betrokkenen worden versterkt. Verplichtingen van verwerkingsverantwoordelijken (hierna verantwoordelijken) en verwerkers worden verzwaard en uitgebreid. Digitale verwerking van persoonsgegevens in een keten of netwerk van verantwoordelijken en verwerkers moet daarom aan strengere eisen voldoen, ook om de risico's voor verantwoordelijken, verwerkers en betrokkenen te kunnen beheersen.

Het blijvend voldoen aan de geldende privacywetgeving is geen sinecure. Een Functionaris voor Gegevensbescherming (FG) is vaak de spil binnen een organisatie in het op orde brengen en ook houden van een adequate gegevensbescherming en privacyhuishouding. De FG is het eerste aanspreekpunt voor de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens (AP). Het gaat bij een contact met een toezichthouder[1] veelal om onduidelijkheden omtrent gegevensbescherming[2] of de afhandeling van een datalek.

De Wet bescherming persoonsgegevens (Wbp) en de Europese verordening gegevensbescherming (Avg) vereisen dat de FG "wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming'.[3] De aard en omvang van het takenpakket vragen minimaal om een post-HBO opleiding. Duthler Academy leidt FG's op in de tweejarige Leergang FG van post-HBO niveau.

Organisaties die gegevensbescherming serieus nemen en een FG hebben aangesteld, willen vaak ook aan de buitenwereld, en meer in het bijzonder aan betrokkenen en het maatschappelijk verkeer, laten zien dat zij gegevensbescherming serieus nemen en aan de uitgangspunten, rechten en verplichtingen van de geldende privacywetgeving voldoen. Dit kan met het Privacy Seal gerealiseerd worden.

---

[1] Veelal hebben organisaties te maken met meerdere toezichthouders met overlappende bevoegdheden. Naast de AP zijn dat bijvoorbeeld AFM, ACM, IGz, DNB.
[2] In deze notitie betekent 'gegevensbescherming': 'bescherming van persoonsgegevens' in de zin van de Wbp. De brede term 'gegevensbescherming' omvat de begrippen 'informatiebeveiliging' (art. 13 Wbp) en wat in het dagelijkse spraakgebruik wordt aangeduid als 'privacy'.
[3] Artikel 63 lid 1 Wbp en artikel 38 lid 5 Avg.

Het Privacy Seal wordt uitgegeven onder gezag van Mind Your Own Business Information, MYOBI.[4] MYOBI is een Trusted Third Party, die voor haar dienstverlening gebruik maakt van de producten en diensten van TTP Associates.[5] Zij maakt gebruik van de professionals van Duthler Associates voor het voeren van het bestuurlijk gesprek met de organisatie die het Privacy Seal aanvraagt. Dat kan een verantwoordelijke of een verwerker in de zin van de Avg zijn.[6] De professionals van Duthler Associates werken nauw samen met de FG van de aanvragende organisatie ter voorbereiding van het bestuurlijk gesprek.

De verdeling van taken, bevoegdheden en verantwoordelijkheden tussen MYOBI, TTP Associates, Duthler Associates, de FG en de vertegenwoordigers van de aanvragende organisatie met betrekking tot het Privacy Seal worden in dit policy document beschreven.

[4] Zie http://www.myobi.eu/nl.
[5] Zie http://www.ttp.associates.
[6] In deze notitie wordt ook wel kortweg de term 'organisatie' gebruikt, in plaats van 'verantwoordelijke of verwerker'.

2. Waarom het Privacy Seal?

Transparantie is een belangrijk uitgangspunt van privacywetgeving. Het gaat er om dat de leiding van een organisatie “accountable” is voor het borgen van gegevensbescherming, privacy en informatiebeveiliging van de bedrijfshuishouding. Met het Privacy Seal bieden organisaties transparantie over het niveau van gegevensbescherming dat keten- en netwerkpartners, de betrokkenen en het maatschappelijk verkeer mogen verwachten. Het Privacy Seal geeft tevens inzicht in de ambities van de organisatie door te tonen binnen welke termijn deze ambities gerealiseerd gaan worden en door te volgen hoe succesvol de organisatie daarin is.
In het geval van het Privacy Seal gaat het erom dat het maatschappelijk verkeer, keten- en netwerkpartners en betrokkenen erop kunnen vertrouwen dat de organisatie zorgvuldig omgaat met gegevensbescherming. MYOBI geeft het Privacy Seal alleen aan organisaties die voldoen aan de criteria voor verlening van het Privacy Seal, dat wil zeggen dat alleen organisaties die serieus bezig zijn met gegevensbescherming het Privacy Seal mogen voeren.

Het Privacy Seal wordt verleend door MYOBI. Duthler Associates verzorgt de Leergang FG aan en beheert het FG Register.

3. Wat is het Privacy Seal?

Het Privacy Seal is een certificaat dat dynamisch uiting geeft aan het niveau van gegevensbescherming dat een organisatie realiseert. Met het Privacy Seal op haar website kan een organisatie laten zien dat men gegevensbescherming op een adequaat niveau realiseert. Organisaties die het Privacy Seal voeren, zijn transparant over het niveau van gegevensbescherming dat betrokkenen en het maatschappelijk verkeer mogen verwachten.

Het recht om het logo met de tekst “Privacy Seal” te gebruiken, wordt door MYOBI verleend aan organisaties die voldoen aan criteria voor zorgvuldige verwerking van persoonsgegevens. MYOBI geeft het Privacy Seal uit en trekt het ook weer in als daar aanleiding voor is.

Het Privacy Seal heeft een dynamisch karakter. Door op het logo te klikken wordt via de website van MYOBI het verantwoordelijkheids- en aansprakelijkheidsdomein van de organisatie getoond. Tevens wordt aangegeven wie als FG is aangesteld. De FG kan aangeven welke informatie over hem zelf wordt getoond. De organisatie kan bepalen welke informatie over de organisatie en het gerealiseerde (en het geambieerde) niveau van gegevensbescherming aan een ieder wordt getoond.

3.1. Criteria op basis waarvan het Privacy Seal wordt verleend

Het recht om het Privacy Seal te gebruiken wordt verleend aan een organisatie (of organisatieonderdeel) als voldaan is aan de volgende voorwaarden:

1. er heeft minimaal één maturity scan en één bestuurlijk gesprek plaatsgevonden, en
2. er is een aspirant FG die de Leergang FG volgt aangesteld bij de organisatie, of
3. er is een door Duthler Academy gecertificeerde FG aangesteld bij de organisatie die is ingeschreven in het FG Register.

3.2. Niveaus van volwassenheid

Organisaties die ernst maken met gegevensbescherming kunnen op het moment van aanvraag van het Privacy Seal verschillende niveaus van volwassenheid of *levels of maturity* ten aanzien van de gegevensbescherming bereikt hebben.

Hieronder beschrijven wij het conceptueel model van zeven *levels of maturity*. Het model beschrijft situaties die zich kunnen voordoen bij organisaties. De hogere *levels of maturity* bouwen in dit model voort op de lagere. Zo moet de organisatie logischerwijs eerst "overzicht en inzicht" hebben om daarna het *level of maturity* "behoorlijk bestuur" te kunnen bereiken.

De *levels of maturity* kunnen zich in de werkelijkheid van organisaties in andere vormen voordoen dan hier beschreven. Daarom vindt ter voorbereiding van het bestuurlijk gesprek een *maturity scan* plaats: een kort onderzoek naar de status van het op dat moment geldende niveau van gegevensbescherming, privacy en informatiebeveiliging op basis van het gehanteerde normenkader. De uitkomsten komen aan de orde in het bestuurlijk gesprek. Het model van de *levels of maturity* biedt de organisatie ook houvast bij het formuleren van ambities. Zie voor een uitgebreide beschrijving van de *levels of maturity* de bijlage.

We onderscheiden de volgende *levels of maturity*:

7. Behoorlijk bestuur
Er is sprake van een heldere beslissingsstructuur voor beleid en aanpak voor gegevensbescherming en privacy als onderdeel van het in standhouden van een verantwoorde bedrijfshuishouding.

6. Georganiseerd zijn
Gegevensbescherming en privacy zijn "ingebouwd" in de organisatie. Niet alleen in de informatiesystemen maar ook in de administratieve organisatie en het handelen van medewerkers, leveranciers en klanten. De werking van de getroffen maatregelen en mechanismen kan getoond worden. De organisatie is "accountable". De organisatie heeft gegevensbescherming zodanig verankerd in de bedrijfsvoering dat gegevensbescherming onderdeel is geworden van het risicomanagement dat een verplicht onderdeel is van de jaarrekening.

5. Eerlijk zaken doen

De betrokkene (klant, medewerker, patiënt of individu) is “in control” over zijn / haar persoonsgegevens. De organisatie heeft de voorwaarden voor eerlijk zaken doen gecreëerd en houdt die ook in stand.

4. Faciliteren van rechten van betrokkene

Actieve en passieve rechten van de betrokkene worden gefaciliteerd. De organisatie kan zich hierover maatschappelijk verantwoorden.

3. Ketenmanagement

Inzicht en overzicht in de verantwoordelijkheden en aansprakelijkheden alsmede in de verwerkingen en de compliance worden uitgebreid naar de bewerkers. Er zijn duidelijke en transparante afspraken tussen verantwoordelijke en verwerkers en tussen verwerkers onderling gemaakt. Er is een basis gelegd voor het voorkómen van bestuurlijke en civielrechtelijke procedures.

2. Overzicht en inzicht

Op systematische wijze zijn de verwerkingen van persoonsgegevens in kaart gebracht. Wijzigingen worden adequaat beheerd. Onderzoeken worden gepland en uitgevoerd. De uitkomsten worden gerelateerd aan het overzicht en inzicht in de verwerkingen.

1. Basic

Er is een besef omtrent gegevensbescherming. Op hoofdlijnen zijn de grenzen van verantwoordelijkheid en aansprakelijkheid in kaart gebracht en er is een FG aangesteld. Het proces van verinnerlijken is gaande.

Daarnaast wordt *maturity level* 0 gehanteerd wanneer het *maturity level* nog niet definitief bepaald kan worden, bijvoorbeeld omdat het aanvraagproces nog niet is afgerond. De verschillende maturity levels worden in het Privacy Seal tot uitdrukking gebracht doordat elk niveau zijn eigen kleur kent.

Afbeelding: Privacy Seal maturity level 5

3.3. Afbakening: wat is het wel en wat is het niet?

Het is wel: inzicht in het niveau van privacy- en gegevensbescherming dat betrokkenen en het maatschappelijk verkeer van de organisatie mogen verwachten.
Het is niet: een "garantie" dat aan alle eisen van het wettelijk kader wordt voldaan en dat er een organisatie is ingericht waarbij taken, bevoegdheden en verantwoordelijkheden binnen regelkringen zijn belegd. Het is geen volledig onderzoek naar opzet, bestaan en werking van beleid en maatregelen rond gegevensbescherming.

Nadere toelichting
De leiding van een organisatie is verantwoordelijk en aansprakelijk voor het opbouwen en in stand houden van een adequate gegevensbescherming. De verantwoordelijkheid strekt zich uit over alle entiteiten die behoren tot de organisatie (kapitaal belang) plus de entiteiten waarin de leiding een belangrijke zeggenschap heeft. Afhankelijk van de gemaakte afspraken kan deze verantwoordelijkheid zelfs tot bij leveranciers en afnemers reiken.

Bij het bestuurlijk gesprek over de toekenning van het Privacy Seal maakt de organisatie het verantwoordelijkheids- en aansprakelijkheidsdomein dat op de organisatie van toepassing is en het privacybeleidsplan inzichtelijk.

Het is noodzakelijk om het verantwoordelijkheids- en aansprakelijkheidsdomein (ook wel: legal entity framework of kortweg LEF) in kaart te brengen om te bepalen wat de scope en reikwijdte van de verantwoordelijkheid voor de gegevensbescherming is. Het resulterende LEF is een krachtig instrument voor de sturing en voor good governance van de organisatie, en ook voor andere terreinen dan dat van de gegevensbescherming.

De organisatie presenteert de strategische doelen en de ambities van de organisatie op de korte en langere termijn op het gebied van gegevensbescherming. Aan de hand hiervan worden “opzet” en “bestaan” van het verantwoordelijkheids- en aansprakelijkheidsdomein en het privacybeleidsplan beoordeeld.

De uitkomsten van het bestuurlijk gesprek worden bij het Privacy Seal gepubliceerd. Het geheel wordt herhaald in een jaarlijkse cyclus die bij voorkeur aansluit op de wettelijke controle van de jaarrekening.

Resultaten

- Organisaties zijn transparant. Hierbij wordt aan de basisgedachte van de wetgever voldaan.
- Er zijn professionals bezig met het privacyvraagstuk. Strategische doelen worden benoemd en tactische mijlpalen worden gehaald. Open en eerlijk.
- Het maatschappelijk verkeer alsmede de toezichthouders worden gefaciliteerd. Wij zouden kunnen zeggen “*managing of expectations*”.
- Er is sprake van “*counseling*”. De situatie op het vlak van gegevensbescherming en privacy wordt doorgenomen en aan de sleutelspelers, verantwoordelijke en FG, wordt raad gegeven.
- De accountant belast met de wettelijke controle van de jaarrekening kan de bevindingen meenemen in zijn afweging in hoeverre de mechanismen effectief functioneren.

3.4. Geldigheidsduur

De overeenkomst voor het gebruik van het Privacy Seal heeft een looptijd van vijf jaar. De overeenkomst wordt daarna steeds stilzwijgend verlengd met een periode van een jaar. Het Privacy Seal is een jaar geldig. Het Privacy Seal mag gedurende het jaar van geldigheid gepubliceerd worden door de organisatie op de eigen website en in marketinguitingen.

Uiterlijk veertien dagen vóór het verstrijken van de geldigheid vindt opnieuw een bestuurlijk gesprek plaats. Het bestuurlijk gesprek heeft ten doel om na te gaan of de geldigheid van het Privacy Seal zonder bezwaar verlengd kan worden door MYOBI, of het *maturity*

level veranderd is, of de doelstellingen zijn bereikt, en welke maatregelen getroffen moeten worden om eventueel een hoger *maturity level* te bereiken.

4. Wat heb ik aan het Privacy Seal?

De organisatie

Door middel van het Privacy Seal toont de organisatie dat men gegevensbescherming op een adequaat niveau realiseert. Met het Privacy Seal kunnen organisaties op compacte wijze weergeven en uitdragen dat men altijd zorgvuldig en transparant omgaat met persoonsgegevens. Betrokkenen zullen eerder kiezen voor een organisatie die uitdraagt dat men ernst maakt met privacy. Toezichthouders zullen eerder geneigd zijn hun controles te richten op organisaties die geen Privacy Seal voeren. Hiermee worden de verwachtingen van betrokkenen en toezichthouders gemanaged.

Het Privacy Seal is een dynamisch geheel dat organisaties stimuleert en faciliteert om steeds een hoger *level of maturity* te bereiken. Welke maatregelen de organisatie daartoe kan nemen, komt aan de orde in het jaarlijkse bestuurlijk gesprek.

De betrokkenen

Voor de personen van wie de organisatie de persoonsgegevens verwerkt (de betrokkenen) maakt het Privacy Seal in een oogopslag duidelijk dat de organisatie de bescherming van hun persoonsgegevens op een adequaat niveau realiseert. Het Privacy Seal is voor betrokkenen een garantie dat zij met eventuele vragen over de verwerking van hun persoonsgegevens terecht kunnen bij de FG van de organisatie. Door het aanklikken van het Privacy Seal op de website van de organisatie, worden de contactgegevens van de FG die is aangesteld getoond.

5. Hoe kom ik aan het Privacy Seal?

Een organisatie komt in aanmerking voor verlening van het Privacy Seal door MYOBI wanneer men voldoet aan de criteria genoemd in paragraaf 3.1. Het Privacy Seal kan aangevraagd worden via de website van MYOBI, http://www.myobi.eu/nl.

5.1. Werkwijze

Maturity scan

Ter voorbereiding van het bestuurlijk gesprek vindt een kort onderzoek (maturity scan) plaats naar de status van het op dat moment geldende niveau van gegevensbescherming, privacy en informatiebeveiliging op basis van het gehanteerde normenkader. De uitkomsten komen aan de orde in het bestuurlijk gesprek.

De maturity scan en het bestuurlijk gesprek worden voorbereid door de FG in samenwerking met professionals van Duthler Associates. De FG voorziet de professionals van documentatie op het terrein van de gegevensbescherming, zoals het verantwoordelijkheids- en aansprakelijkheidsdomein dat op de organisatie van toepassing is en het privacybeleidsplan (indien aanwezig).

Bestuurlijk gesprek

Na de maturity scan vindt een bestuurlijk gesprek plaats tussen de professionals van Duthler Associates met de FG én de vertegenwoordiger (portefeuillehouder gegevensbescherming in de raad van bestuur of directie) van de organisatie die het Privacy Seal aanvraagt.

Het doel van het bestuurlijk gesprek is na te gaan wat de actuele stand van zaken van gegevensbescherming is binnen de organisatie en of het Privacy Seal verleend kan worden. De *levels of maturity* dienen in het bestuurlijk gesprek als gespreksthema's.

Verder dient het bestuurlijk gesprek om te bepalen welk ambitieniveau de organisatie heeft en wat er voor nodig is om vanuit de intenties van de organisatie de doelen te bereiken. Op basis van de documentatie en de uit het bestuurlijk gesprek verkregen informatie wordt het verantwoordelijkheids- en aansprakelijkheidsdomein bepaald en ingeregeld in

het LEF. Als aan de geldende criteria (zie paragraaf 3.1) wordt voldaan, wordt een Privacy Seal verstrekt.

Vervolgens
Bij de volgende bestuurlijk gesprekken is sprake van "counseling". De situatie op het vlak van gegevensbescherming en privacy wordt doorgenomen en aan de sleutelspelers, verantwoordelijke en FG, wordt raad gegeven. Verantwoordelijken kunnen ambitieniveaus vaststellen om gaandeweg hogere niveaus te bereiken. Het moment van rapporteren wordt zodanig gekozen dat de accountant belast met de wettelijke controle van de jaarrekening de bevindingen kan meenemen in zijn afweging in hoeverre de mechanismen effectief functioneren.

De onderwerpen die aan de orde komen in het bestuurlijk gesprek variëren al naar gelang het *maturity level* dat de organisatie op dat moment bereikt heeft. Thema's als "ketenmanagement", "overzicht en inzicht" hebben een ander karakter dan het thema "goed bestuur". De adviezen die voortkomen uit het bestuurlijk gesprek, groeien mee met het *maturity level*. Op de lagere niveaus kan het advies bijvoorbeeld luiden om een Privacy Impact Assessment te doen, omdat de aanschaf van een nieuw informatiesysteem wordt overwogen. Op de hogere niveaus zou het advies kunnen luiden om in het kader van de jaarrekening de accountant en de Raad van Commissarissen te betrekken bij de beoordeling van het risicomanagement rond de gegevensbescherming.

Technische en operationele zaken
Technische en operationele zaken rond het Privacy Seal worden uitgevoerd. De aangestelde FG wordt in het FG Register van Duthler Academy opgenomen. De FG kan aangeven welke informatie over hem zelf gepubliceerd mag worden. De organisatie bepaalt welke informatie over de organisatie gepubliceerd mag worden. Vervolgens wordt de koppeling tussen het verantwoordelijkheidsdomein en de FG gemaakt en is het Privacy Seal geactiveerd.

Bij het bestuurlijk gesprek worden afspraken gemaakt met de verantwoordelijke en de FG. Van de uitkomsten van de gesprekken wordt een rapport van bevindingen opgesteld dat,

na een check op feitelijke juistheid door de organisatie, onder het Privacy Seal wordt gepubliceerd.

In het bestuurlijk gesprek wordt aangesloten bij de wettelijke basis van good governance, BW2:391.5 waarbij plan, financiering en realisatie centraal staan.
Er wordt een koppeling gemaakt tussen het verantwoordelijkheidsdomein van de organisatie met het toezichtdomein van de FG c.q. aspirant FG (uitgangspunt).

5.2. Verdeling taken en verantwoordelijkheden

De verantwoordelijke

- moet blijvend voldoen aan de criteria voor het Privacy Seal;
- bepaalt het ambitieniveau; en
- betaalt voor het gebruik van het Privacy Seal.

De FG

- houdt toezicht op de gegevensbescherming; en
- bereidt het bestuurlijk gesprek voor.

MYOBI

- verleent het Privacy Seal;
- zorgt voor de interactieve koppeling met FG Register en LEF;
- zorgt voor de uitvoering van de maturity scan en het bestuurlijk gesprek, eventueel met inschakeling van Duthler Associates; en
- stelt het rapport van bevindingen op dat gepubliceerd wordt onder het Privacy Seal.

5.3. Criteria voor intrekking van het Privacy Seal

MYOBI kan het recht om het Privacy Seal te gebruiken beëindigen wanneer:

1. aanbevelingen van de FG (of aspirant FG) of bevindingen gemeld in het bestuurlijk gesprek onvoldoende leiden tot maatregelen, of
2. het privacybeleidsplan niet wordt uitgevoerd, of
3. de organisatie niet langer voldoet aan de criteria die gelden voor de toekenning van het Privacy Seal (zie paragraaf 3.1).

6. Hoe past het Privacy Seal bij de privacywet- en regelgeving?

Het Privacy Seal sluit aan bij de reeds in werking getreden Europese wetgeving.

In artikel 42 van de Avg staat bepaald dat de lidstaten, de toezichthoudende autoriteiten, het Comité en de Commissie de invoering van certificeringsmechanismen voor gegevensbescherming en gegevensbeschermingszegels en –merktekens bevordert. Met de zegels en merktekens kan worden aangetoond dat verwerkingsverantwoordelijken en verwerkers bij verwerkingen in overeenstemming met deze verordening handelen. Het Privacy Seal kan worden opgevat als zo'n gegevensbeschermingszegel.

De Avg gaat er van uit dat de certificering vrijwillig is en toegankelijk via een transparant proces.[7] Certificering doet niets af aan de verantwoordelijkheid van de verwerkingsverantwoordelijke of verwerker om de verordening na te leven en laat de taken en bevoegdheden van de toezichthoudende autoriteiten onverlet.[8]

De Avg gaat er verder van uit dat een certificaat wordt afgegeven door een certificerend orgaan of door de AP.[9] MYOBI kan worden opgevat als zo'n certificerend orgaan. De lidstaten zorgen er voor dat het certificerend orgaan wordt geaccrediteerd door de AP of door de nationale accreditatie-instantie die is aangewezen in overeenstemming met de betreffende Europese verordening[10], in overeenstemming met EN-ISO/IEC 17065/2012 en met de aanvullende eisen die door de AP zijn vastgesteld. De AP heeft nog geen duidelijkheid gegeven of zij zelf of een nationale accreditatie-instantie gaat accrediteren en op grond van welke criteria dat dan gebeurt. MYOBI houdt dit nauwlettend in de gaten en zodra de duidelijkheid er is zal zij kenbaar maken of en op welke wijze zij opgaat voor accreditering.

---

[7] Zie het derde lid van artikel 42 Avg.

[8] Zie het vierde lid van artikel 42 Avg.

[9] Zie het vijfde lid van artikel 42 Avg.

[10] Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30).

MYOBI heeft het Privacy Seal zodanig ingericht, dat zij is voorbereid op een eventuele accreditatie om de privacy seals uit te mogen geven. De privacy seals die eerder dan de accreditatie worden uitgegeven, blijven hun waarde behouden. MYOBI behoudt zich het recht voor om, wanneer dat nodig is, deze policy en de algemene voorwaarden van het Privacy Seal programma aan te passen.

7. De rol van de FG

De FG is het eerste aanspreekpunt voor de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens (AP). Het gaat dan veelal om onduidelijkheden omtrent gegevensbescherming of de afhandeling van een datalek. Binnen de organisatie is de FG de spil in het op orde brengen en ook houden van een adequate gegevensbescherming en van de privacyhuishouding.

De aanstelling van een door Duthler Associates gecertificeerde FG (of een aspirant FG die de Leergang FG volgt) in de organisatie is een voorwaarde voor de verlening van het Privacy Seal. Door een FG aan te stellen toont een organisatie dat men gegevensbescherming op een adequaat niveau realiseert. De FG neemt deel aan het bestuurlijk gesprek over het Privacy Seal met de verantwoordelijke.

De FG c.q. aspirant FG houdt toezicht op de gegevensbescherming binnen de organisatie en adviseert de verantwoordelijke over de te nemen maatregelen om te zorgen dat de verwerking van persoonsgegevens binnen de organisatie op een correcte manier plaatsvindt. De FG die door de Duthler Associates is gecertificeerd beschikt over de voor de functie benodigde kennis en vaardigheden op post hbo-niveau en wordt ingeschreven in het FG Register. Voor behoud van de inschrijving in het FG Register volgt de FG het PE Programma van de Duthler Academy. De aspirant FG is in opleiding bij Duthler Academy en zodoende op weg naar dat niveau. Beide typen FG's kunnen gebruik maken van de kennis en ervaring die gebundeld is in de "community" van FG's van de Duthler Academy. Duthler Academy is een onderdeel van Duthler Associates.

8. Relatie met het FG Register en het FG Cluster

FG's in opleiding en door Duthler Academy gecertificeerde FG's worden opgenomen in het FG Register van Duthler Associates. De nascholing van FG's verloopt via het PE Programma van Duthler Academy. Duthler Academy bewaakt de kwaliteit van de opleiding en het PE Programma. Om de inschrijving in het FG Register te behouden moet de FG voldoen aan de voorwaarden van het PE programma.

FG's en aspirant FG's hebben toegang tot elkaars contactgegevens en kunnen elkaar raadplegen door middel van het FG Cluster, de "community" van FG's. Op deze manier vormt het FG Cluster een extra kwaliteitswaarborg van het Privacy Seal. Duthler Associates faciliteert en modereert het FG Cluster.

9. Relatie met Trusted Third Party en TTP-policy

Een TTP ziet toe op de uitvoering van afspraken in het kader van gegevensuitwisseling tussen partijen in een keten of netwerk. Het Privacy Seal is een voorwaarde voor deelname aan een keten of netwerk waar een TTP de regie voert. Het Privacy Seal toont aan keten- en netwerkpartners, betrokkenen en derden dat men kan vertrouwen op een bepaald niveau van gegevenbescherming.

Compliance vereist dat er regie gevoerd wordt over de gehele keten of het netwerk van betrokkenen, verantwoordelijken, verwerkers en subverwerkers. De TTP is de onafhankelijke en onpartijdige entiteit die er op toeziet dat de afspraken inzake gegevensbescherming in de keten en/of het netwerk worden nageleefd. De TTP werkt normerend, controlerend, faciliterend en de-escalerend voor de verwerkingen in een keten of netwerk.

Voor de kwaliteit van de gegevensverwerking in de gehele keten of het netwerk is het noodzakelijk dat keten- en netwerkpartners een gemeenschappelijk niveau van gegevensbescherming hebben. Door middel van het Privacy Seal brengen keten- en netwerkpartners dat gemeenschappelijk niveau van gegevensbescherming tot uiting op hun websites.

Voor de TTP is de aanwezigheid van een Privacy Seal bij een keten- of netwerkpartij een voorwaarde voor aansluiting bij de TTP. Het Privacy Seal verschaft de TTP een basis voor diens normerende, controlerende, faciliterende en de-escalerende functies. Keten- of netwerkpartijen met een Privacy Seal hebben een FG aangesteld. Wanneer actie vereist is, zoals bij incidenten, is de FG voor de TTP het deskundige aanspreekpunt bij de keten- of netwerkpartij.

De TTP organiseert de gegevensbescherming en de borging in de keten door met keten- en netwerkpartijen *maturity levels* af te spreken. Deze *maturity levels* zijn gedefinieerd in de bijlage. De TTP bepaalt in overleg met keten- en netwerkpartijen het voor de keten of het netwerk geldende minimale *maturity level* en bepaalt daarmee aan welke criteria moet worden voldaan.

10. Relatie met het Legal Entity Framework (LEF)

Op basis van de documentatie en de uit het bestuurlijk gesprek verkregen informatie wordt het verantwoordelijkheids- en aansprakelijkheidsdomein bepaald en ingeregeld in het LEF. LEF management is het op gestructureerde wijze in beeld brengen van de corporate family en / of de verbonden partijen. Overzicht en inzicht in de formeel-juridische structuur van een organisatie, de samenwerkingen, de verwerkers aan wie activiteiten zijn uitbesteed en andere verbonden partijen is nodig om het verantwoordelijkheids- en aansprakelijkheidsgebied van de Raad van Bestuur en Raad van Commissarissen af te kunnen grenzen. Daarbij wordt gebruik gemaakt van het SBC Managementsysteem.

Het SBC Managementsysteem maakt het tevens mogelijk om overzicht en inzicht in gegevensverwerkingen en in de privacy- en veiligheidshuishouding van een organisatie te verkrijgen en te behouden. Het SBC Managementsysteem biedt ook ondersteuning bij de afhandeling van datalekken. Het SBC Managementsysteem geeft de verantwoordelijke, raad van bestuur en raad van commissarissen, volledig inzicht in het verantwoordelijkheidskader welke is opgebouwd uit overzicht en inzicht in de corporate family en volledig is gedocumenteerd en wordt onderhouden in SBC LEF | LEM. Daarnaast biedt dit overzicht en inzicht in alle verwerkingen van (privacygevoelige) gegevens, de processen waarin deze

worden uitgevoerd en de systemen die deze processen aansturen, vastgelegd en onderhouden in SBC Privacy.

11. Overige informatie en vragen

Voor overige informatie en vragen kunt u contact opnemen met mr. Ans Duthler:

Frankenslag 137

2582 HH Den Haag

Telefoon +31 (70) 392 2209

Mail info@myobi.nl

Meer informatie over de rol van de TTP en de TTP policy is op aanvraag beschikbaar.

Bezoek http://www.myobi.eu/nl voor meer informatie over het Privacy Seal.

Bezoek http://www.ttp.associates voor meer informatie over de TTP.

Bezoek www.sbrpowerhouse.nl voor meer informatie over het SBC Managementsysteem.

Bijlage: Maturity levels

Levels	Omschrijving	Klein	Middel	Groot
0. **Onbepaald**	Het maturity level kan nog niet definitief bepaald worden, bijvoorbeeld omdat het aanvraagproces nog niet is afgerond.			
		>	>	>

Bijlage: Maturity levels

Levels	Omschrijving	Klein	Middel	Groot
1. **Basic**	Er is een besef omtrent gegevensbescherming, privacy en beveiliging. Op hoofdlijnen zijn de grenzen van verantwoordelijkheid en aansprakelijkheid in kaart gebracht en zover nodig is een FG aangesteld of in de functie voorzien. Het proces van verinnerlijken is gaande.	De organisatie heeft de grenzen van het domein waarvoor de organisatie verantwoordelijk en aansprakelijk is, bepaald door te beschrijven met welke 'legal entities' de organisatie verbonden is. De organisatie bouwt deskundigheid op over gegevensbescherming en informatiebeveiliging. De organisatie werkt aan het privacybewustzijn van de medewerkers. In het bestuurlijk gesprek wordt bepaald welk ambitieniveau de organisatie heeft en wat er voor nodig is om vanuit de intenties van de organisatie de doelen te bereiken. Resultaten van het bestuurlijk gesprek worden gepubliceerd.		
		> De corporate family is op hoofdlijnen vastgelegd. Er wordt gebruik gemaakt van een subset van het SBC Management Systeem, dat in het kader van het Privacy Seal ter beschikking wordt gesteld. > De functie van FG is (extern) belegd en de scope is gegevensbescherming en informatiebeveiliging. > Op basis van "op weg naar huis"-bijeenkomsten en of e-learning modules wordt de kennis op niveau gebracht. > De uitkomsten van het bestuurlijk gesprek zijn openbaar en zijn vooral gericht op de "awareness" van de leiding en de accountant, belast met het samenstellen van de jaarrekening, door deze te voorzien van de minimaal noodzakelijke informatie.	> De corporate family is in kaart gebracht. Er wordt gebruik gemaakt van een subset van het SBC Management Systeem, dat in het kader van het Privacy Seal ter beschikking wordt gesteld. > Een FG is aangewezen of de functie wordt (extern) ingevuld. Kennisniveau van FG ligt op het niveau van de FG Leergang. Hierbij wordt aansluiting gezocht bij de activiteiten die worden uitgevoerd in het kader van gegevensbescherming en informatiebeveiliging. > In de organisatie wordt de "awareness" verkregen door het instellen van een projectgroep, presentaties aan medewerkers en vertegenwoordigers van bewerkers en inzetten van e-learning modules waarbij het kennisniveau wordt getoetst. > Het bestuurlijk gesprek is gericht op het verkennen van de verantwoordelijkheden en aansprakelijkheden alsmede het bepalen van de stappen die nodig zijn de aansprakelijkheids- en kostenrisico's van niet compliantgedrag te beheersen. Uitkomsten van het overleg zijn openbaar en ook met name gericht op de accountant belast met het samenstellen en of	> De corporate family en belangrijke verbonden partijen zijn in kaart gebracht. In eerste aanleg wordt gebruik gemaakt van een subset van het SBC Management Systeem, dat in het kader van het Privacy Seal ter beschikking wordt gesteld. De toepassing van een organisatie breed managementsysteem waarin de gedelegeerden de noodzakelijke informatie voor vastleggingen van gegevensbescherming en beveiliging, onder toezicht van de FG, kunnen vastleggen wordt nader onderzocht. > Een FG is aangewezen vanuit eigen organisatie, in dienst genomen of uit het FG-Cluster van Duthler Academy aangesteld. Het kennisniveau van de FG ligt op het niveau van de FG Leergang. > Kennisopbouw wordt in de organisatie in een project onder leiding van een lid van de Raad van Bestuur/RvC en FG structureel en aantoonbaar opgepakt. Als onderdeel van de beleidscyclus wordt gegevensbescherming, privacy en informatiebeveiliging als een prioriteit opgenomen. De FG en een lid van de Raad van bestuur en/of Raad van commissarissen / toezicht is hierbij betrokken. > Wij verwachten dat grote organisaties snel de behoefte hebben aan volgend "maturity level". Hierbij planmatig te

Bijlage: Maturity levels

Levels	Omschrijving	Klein	Middel	Groot
			de controle van de jaarrekening.	werk gaan. Het bestuurlijk gesprek is gericht op de uitkomsten van de beleidsvorming, verkennen van de verantwoordelijkheden en aansprakelijkheden alsmede het bepalen van de stappen die nodig zijn de aansprakelijkheids- en kostenrisico's van niet compliantgedrag te beheersen. Uitkomsten van het overleg zijn openbaar en ook met name gericht op de accountant belast met de controle van de jaarrekening.

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
2. **Overzicht en inzicht**	Uitgaande van het basis niveau wordt op systematische wijze per entiteit de verwerkingen van persoonsgegevens in kaart gebracht, gedocumenteerd en worden wijzigingen adequaat beheerd. Er wordt een begin gemaakt met privacy en security accounting (PSA). Regelkringen worden aantoonbaar gesloten. Onderzoeken (PIA's en Audits) worden gepland, uitgevoerd en gedocumenteerd. Uitkomsten van interne controle worden systema-	Kennis en vaardigheid omtrent privacy en security accounting wordt opgedaan. Onder aansturing van de leiding wordt beleid omtrent gegevensbescherming, privacy en informatiebeveiliging geformuleerd, maturity levels in een tijdsperspectief gekozen en middelen vrijgemaakt om het beleid ook daadwerkelijk uit te voeren. Het voldoen aan de documentatieverplichting wordt geplaatst in een managementcyclus. Het al dan niet adequaat zijn van de getroffen beheers- en beveiligingsmaatregelen kan op basis van de gedocumenteerde verwerkingen worden aangetoond. In hoeverre de organisatie de aansprakelijkheids- en kostenrisico's kan beheersen wordt afgelezen aan de hand van het vastgelegde bewijs omtrent de effectieve werking van de getroffen maatregelen. Afhankelijk van de aard en omvang van de organisatie wordt voor de privacy en security accounting gebruik gemaakt van adequate hulpmiddelen. De organisatie beschikt over een adequaat model bewerkersovereenkomst dat door een advocaat toereikend wordt gevonden. Wij kunnen zeggen dat de organisatie op zekere hoogte weerbaar is. Op basis van de uitkomsten van de managementcyclus en de interne controle kan de leiding van de organisatie op dit niveau aangeven "accountable" te zijn. Het instrument Privacy Impact Assessment (PIA) wordt aanvullend ingezet voor risicogebieden. De uitkomsten van het bestuurlijke gesprek bieden ketenpartners meer zekerheid omtrent de betrouwbaarheid van de uitspraak van de leiding. De externe (IT-)auditor wordt een startpunt geboden een auditopdracht aan te nemen (de organisatie is "auditability" voor de accountant).		
		> Het overzicht van de corporate family wordt aangevuld met de documentatie van alle verwerkingen. Hierbij wordt de samenhang met processen, deelprocessen en activiteiten duidelijk. Afhankelijk van het aantal verwerkingen kan behoefte ontstaan voor een gemeenschappelijk taxonomie-gedreven accounting- en managementsysteem. > De managementcyclus wordt op gang gebracht door het verzamelen van bewijs dat gedocumenteerde beheers- en beveiligingsmaatregelen in de verwerkingen effectief hebben gewerkt. Een functionaris die de FG functie vervult, coördineert	> Het overzicht op hoofdlijnen in de corporate family wordt nader ingevuld en uitgebreid met de belangrijkste verbonden partijen. Vervolgens wordt per entiteit voldaan aan de documentatieverplichting van alle verwerkingen. De samenhang tussen entiteiten, verwerkingen, (deel-) processen en informatiesystemen wordt in kaart gebracht en expliciet vanuit een tijdsperspectief gelegd en beheerd. Bij het documenteren worden onder andere de maatregelen en mechanismen, bewaartermijnen en risico-classificatie vastgelegd. > De maatregelen van interne controle, gericht op het vaststellen en vastleggen van de effectieve werking beheersmaatregelen wordt gekoppeld aan de documentatie van verwerkingen. Er is sprake van een	> De corporate family alsmede de verbonden partijen zijn in kaart gebracht. Er wordt een professioneel informatiesysteem voor legal entity management (LEM) toegepast (mogelijke optie is SBC Management Systeem dat in het kader van het Privacy Seal ter beschikking is gesteld uitbreiden voor het onderhavige beheersgebied). > Een FG is aangewezen vanuit de eigen organisatie, in dienst genomen of uit het FG-Cluster van Duthler Academy aangesteld. Het kennisniveau van de FG ligt op het niveau van de FG Leergang. Kennisopbouw wordt in de organisatie projectmatig en onder leiding van de FG structureel en aantoonbaar opgepakt. Er ontstaat een netwerk van gedelegeerden / privacy en security contactpersonen. Als onderdeel van de beleidscyclus wordt gegevensbescherming en privacy als een prioriteit opgenomen. De leiding van de entiteit tekent af op

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
	tisch vastgelegd en gerelateerd aan de gedocumenteerde verwerkingen van persoonsgegevens. Effectieve werking van de getroffen beheers- en beveiligingsmaatregelen worden vastgesteld.	dit en faciliteert. > Het bestuurlijk gesprek wordt opgenomen in een (jaarlijkse) managementcyclus.	netwerk van privacy en security coördinatoren ter ondersteuning van de FG. De leiding van de entiteiten tekent af op gegevensbescherming, privacy en informatiebeveiliging. De FG en een lid van de RvB/RvC is hierbij betrokken. > De omvang van de organisatie maakt het toepassen van een taxonomie-gedreven managementsysteem sterk aan te bevelen. In veel situaties zelfs noodzakelijk. Het vastleggen van “evidence” omtrent de effectieve werking van de getroffen maatregelen wordt systematisch (en bij voorkeur geautomatiseerd en op basis van een taxonomie) vastgelegd en beoordeeld. > De uitkomsten van PIA’s en Audits (inclusief de werkzaamheden van de externe (IT-)auditor) worden opgenomen in een in een professionele administratie of (taxonomie gedreven SBC) systeem. PIA’s worden uitgevoerd op kritische en nieuwe verwerkingen. De FG coördineert en faciliteert en is verantwoordelijk voor het documenteren van de verwerkingen. > Het bestuurlijk gesprek gaat over het realiseren van beleid en er wordt gesproken over volwassenheid- en ambitieniveau. Het overleg wordt opgenomen in een (jaarlijks) managementcyclus.	gegevensbescherming, privacy en informatiebeveiliging. De FG en een lid van de raad van commissarissen / toezicht is hierbij betrokken. > Er ontstaat snel behoefte een organisatie breed interne controle systeem waarin management- en accounting alsmede LEM zijn geïntegreerd. Voldoen aan de documentatieplicht alsmede het vastleggen van bewijs dat getroffen maatregelen effectief hebben gewerkt worden in het systeem vastgelegd (zoveel als mogelijk met geautomatiseerde koppelingen). De samenhang tussen de documentatie van verwerkingen en het bewijs van effectieve werking in de administratieve organisatie wordt bewaakt. > Het systeem ondersteunt ook de organisatie van gedelegeerden / contactpersonen met het uitvoeren van hun taken. Het systeem is de basis voor het organiseren van de interne controle (op entiteit en geconsolideerd niveau) en het kunnen afleggen van verantwoording aan het maatschappelijk verkeer. Wij verwachten dat grote organisaties snel de volgende “maturity” stap zullen zetten. > Het bestuurlijk gesprek is gericht op de uitkomsten van de beleidsvorming, verkennen van de verantwoordelijkheden en aansprakelijkheden alsmede het bepalen van de stappen die nodig zijn de aansprakelijkheids- en kostenrisico’s van niet compliantgedrag te beheersen. Uitkomsten van het gesprek zijn openbaar en ook met name gericht op de accountant belast met de controle van de jaarrekening.

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
3. **Keten-/ management**	Uitgaande van overzicht en inzicht wordt aan keten, of liever gezegd netwerkmanagement invulling gegeven. Hierbij gaat de interne controle verder dan de grenzen van de eigen organisatie. Dit met als doel de aansprakelijkheids- en kostenrisico's (die voort kunnen vloeien uit zowel publiek- als civielrechtelijke complicaties) beheersbaar te maken en te houden. Over de uitkomsten transparant zijn naar het maatschappelijk	Naarmate er meer ervaring is opgedaan met privacy en security accounting (PSA) en de verwerkingen van persoonsgegevens in kaart zijn gebracht zal het ketenmanagement van de organisatie gericht zijn op het in standhouden van het overzicht en inzicht alsmede het systematisch vastleggen van bewijs omtrent de effectieve werking van de getroffen beheers- en beveiligingsmaatregelen. Verbonden partijen (waaronder alle bewerkers) zijn opgenomen in de corporate family. Stap voor stap kunnen maatregelen van interne controle worden ingesteld en zal periodiek hierover aan de leiding worden gerapporteerd. Speciale aandacht is er voor het organiseren van het opvangen van incidenten zoals bedoelt in meldplicht datelekken / beveiligingsincidenten. Het ketenmanagement gaat de grenzen van de eigen organisatie voorbij. De interne afspraken omtrent taken, bevoegdheden en verantwoordelijkheden van functionarissen moeten tussen ketenpartners opnieuw gemaakt worden. Eén en ander kan worden geregeld met een adequate bewerkersovereenkomst waarin een vorm van een kettingbeding is voorziet. De meldplicht datalekken kan immers verstrekkende gevolgen hebben voor de ketenpartners. Een adequate en interoperabele documentatie (waaronder bewijs van effectieve werking) van verwerkingen en meldingen zijn essentieel verweer te voeren tegen de toezichthouders en of onderling. Naarmate het netwerk omvangrijk is of de aard van de persoonsgegevens dat vragen kan een proactieve Trusted Third Party (TTP) sterk de-escalerend werken bij het oplossen van calamiteiten.		
		> De onder de verantwoording van de verantwoordelijke / bewerker uitgevoerde verwerkingen worden adequaat gemonitord en de uitkomsten worden systematisch vastgelegd. > Contracteren vindt plaats op basis van een bewerkersovereenkomst met een vorm van kettingbeding. Er wordt aangesloten bij algemeen geaccepteerde standaarden. > Privacy / security incidenten worden gesignaleerd en conform de afspraken in een policy gedocumenteerd en afgewikkeld. De FG, in samenspraak met de leiding, zet specialisten bij incidenten	> Het overzicht en inzicht in de verwerkingen wordt onder verantwoordelijkheid van de FG bijgehouden. De verwerkingen worden adequaat gemonitord. Bewijs van adequaat functioneren en eventuele incidenten worden taxonomie-gedreven vastgelegd. > Met alle bewerkers / (sub-)bewerkers zijn bewerkersovereenkomsten met een vorm van kettingbeding afgesloten. De bewerkersovereenkomsten zijn wederkerig en policy gedreven. Voor het contracteren van een nieuwe bewerker wordt een PIA uitgevoerd. De uitkomsten zijn richtinggevend voor de te maken afspraken (het kan voorkomen dat de bewerker niet aan de criteria kan voldoen). > Privacy / security incidenten worden gesignaleerd en conform de afspraken gedocumenteerd en afgewik-	> Uitgaande van overzicht en inzicht in alle verwerkingen in een gedistribueerde omgeving van de corporate family van een organisatie ziet de FG toe dat de administratie van de gegevensbescherming en privacy "up to date" is en blijft. Het toepassen van de "accounting principles" en de administratie vallen rechtstreeks onder verantwoordelijkheid van de FG. Geregeld zal de FG onderzoek uitvoeren naar de betrouwbaarheid van de administratie en in het kader van afspraken met de audit committee zal de FG vragen onderzoek te laten verrichten door interne of externe auditors. > Met alle bewerkers / (sub-)bewerkers zijn bewerkersovereenkomsten met een vorm van kettingbeding. Alle bewerkersovereenkomsten zijn policy gedreven; bij voorkeur TTP policy gedreven. Bij het contracteren van nieuwe bewerkers wordt een PIA uitgevoerd. De uitkomsten zijn

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
	verkeer en misschien wel belangrijker naar de deelnemers in het netwerk.	en/of verzoeken van de toezichthouders in. Op basis van “op weg naar huis”-bijeenkomsten en of e-learning modules wordt de kennis op niveau gebracht. De organisatie gaat de “stress levels” na en doet mee aan “simulaties”. > Het bestuurlijk gesprek staat in het teken van beperken van aansprakelijkheids- en kostenrisico’s.	keld. De FG zet, in samenspraak met de leiding, specialisten in bij incidenten en of verzoeken van de toezichthouders. In de organisatie wordt toetsbare kennis opgebouwd bij sleutelpersonen in de organisatie. Hiermee wordt het mogelijk dat effectief gebruik kan worden gemaakt van (bijvoorbeeld door een TTP) beschikbaar gestelde informatie. Het overgrote deel van de incidenten / datalekken kan door de organisatie zelf worden afgehandeld. Voor specialistische of risicovolle casussen kan de FG, in samenspraak met de leiding, specialisten inzetten. De stress bestendigheid van het response team bij incidenten / datalekken wordt door de FG getest met relevante “simulaties”. Dit wordt georganiseerd in samenhang met het netwerk van verantwoordelijken en (sub-) bewerkers. Het bestuurlijk gesprek staat in het teken van beperken van kosten en aansprakelijkheidsrisico’s. De doortastendheid van de FG is daarbij belangrijk. De opdracht en de resultaten worden gepubliceerd.	richtinggevend voor de te maken afspraken (het kan voorkomen dat de bewerker niet aan de criteria kan voldoen). Bij voldoende omvang kan de organisatie besluiten “binding corporate rules”, (BCR’s) op te stellen en toe te passen. Dit niveau van volwassenheid (TTP policy gedreven bewerkers-overeenkomst) is daarvoor een geschikt moment om een start te maken. > Op basis van professionele producten en diensten wordt proactief gezocht naar privacy/security incidenten. Deze kunnen zich op verschillende niveaus van de organisatie voordoen. De gesignaleerde incidenten worden conform de afspraken in de policy gedocumenteerd, geanalyseerd en afgewikkeld. Bij het afwikkelen worden ook de entiteiten in het netwerk gewaarschuwd voor incidenten die de groep of keten aangaan. Voor het afwerken van incidenten of beantwoorden van vragen van toezichthouders wordt een getraind crisisteam samengesteld. Een lid van de raad van bestuur leidt een dergelijk team en externe specialisten kunnen aan het team worden toegevoegd. De FG ziet toe op het proces en zorgt dat de documentatie juist en volledig is. In de organisatie wordt toetsbare kennis opgebouwd bij sleutelpersonen in de organisatie. Hiermee wordt het mogelijk dat effectief gebruik kan worden gemaakt van beschikbaar gestelde informatie. De stress bestendigheid van het crisisteam bij incidenten / datalekken wordt door de FG getest met relevante “simulaties”. Dit wordt georganiseerd in samenhang met het netwerk van verantwoordelijken en

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
				(sub-)bewerkers. > Het bestuurlijk gesprek staat in het teken van beperken van kosten en aansprakelijkheidsrisico's. Transparant zijn vormt een uitgangspunt voor compliance. De FG moet in staat zijn de organisatie en het vraagstuk te overzien.

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
4. **Faciliteren van rechten van betrokkene**	Uitgaande van adequaat ketenmanagement worden de verplichtingen van de verantwoordelijke / bewerker georganiseerd. Het complement hiervan zijn de rechten van de betrokkene. Tevens wordt invulling gegeven aan de andere verplichtingen zoals het organiseren van een passend beveiligingsniveau, toepassen van PbD * 2, uitvoeren van PIA's, onder voorwaarden toepassen van profiling.[11]	De administratieve organisatie dient op dit niveau zodanig te zijn ingericht dat het te allen tijde kan voldoen aan een verzoek van een betrokkene om informatie, correctie, wijziging of vernietiging van de persoonsgegevens van de betrokkene te faciliteren. De administratieve organisatie moet zodanig zijn dat de systemen en procedures dit mogelijk maken. Het proces voor het uitoefenen van deze rechten geeft zekerheid omtrent de juiste identiteit van de betrokkene aan wie informatie wordt verstrekt en ook dat de informatie tijdig is aangeleverd. Veelal is de verantwoordelijke het eerste aanspreekpunt voor vragen van de betrokkene en moet de bewerker kunnen omgaan met deze vragen. Het is niet ondenkbaar dat vanuit het netwerk een TTP processen faciliteert. Doel van een dergelijk opzet is het veiligstellen van bewijs voor het afwerken van processen ten behoeve van betrokkene. Wij spreken dan over een "inline" TTP.[12] De andere verplichtingen van de verantwoordelijke en of bewerker worden professioneel en effectief afhankelijk van de stand van de techniek georganiseerd.		
		> Voorzien in "gecontroleerde" transparantie aan betrokkene en andere leden in het netwerk kan voor een kleine entiteit behoorlijk wat voeten in aarde hebben. In de praktijk bestaat een afhankelijkheid met middel grote en grote organisaties. > De FG zal de verzoeken in behandeling nemen, zorgen dat de wettelijke termijnen worden gehaald en dat de noodzakelijke documentatie van de verzoeken wordt vastgelegd. De FG maakt steeds de afweging in hoeverre secundaire overwegingen aan de verzoeken ten grondslag liggen. > De FG houdt de formele actualiteiten bij	> Onder leiding van de FG wordt nagegaan op welke wijze voorzien wordt / kan worden in de verplichtingen van de verantwoordelijke / bewerker. Het overzicht en inzicht in de documentatie vormt daarbij een goede basis. Met een centraal opgestelde dienst die gebruik maakt van de door een TTP ter beschikking gestelde taxonomieën kunnen verzoeken worden afgehandeld en worden gedocumenteerd. Speciale aandacht vraagt de rechten van betrokkenen op doorhaling, correctie en vergeten te worden. > De FG zal toezien op het hanteren van de afgesproken "vernietigingstermijnen" van verwerkingen. Een medewerker zal namens de FG de verzoeken in behandeling nemen, zorgen dat de wettelijke termijnen worden gehaald en dat de noodzakelijke	> Onder verantwoordelijkheid van de leiding wordt voorzien in de verplichtingen van de verantwoordelijke en bewerker. De aangewezen contactpersonen zijn de "linking pins" naar het compliance cluster met de FG en ISO. De uitdaging voor grote organisaties is overzicht te krijgen en houden op de verzoeken van de betrokkenen en de wijze waarop deze verzoeken door de verschillende entiteiten zijn afgedaan. De contactpersonen (gedelegeerde van de FG) ziet toe op deze processen en grijpt in als dat noodzakelijk is. Het ligt voor de hand dat de leiding een centraal opgestelde dienstverlening inricht die verzoeken van betrokkene door het netwerk van contactpersonen taxonomie-gedreven en op basis van een vastgestelde mores laten afhandelen. De door een TTP beschikbaar gestelde taxonomieën zijn goed toepasbaar. > Met de verbonden partijen en in het bijzonder de bewerkers zijn in de bewerkersovereenkomst afspraken gemaakt over

[11] PbD * 2 is de afkorting voor "privacy by design" en "privacy by default". Kort en goed wordt de wet- en regelgeving in systemen ingebouwd in plaats van het toepassen van de wet- en regelgeving.

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
		en gaat na welke maatregelen verplicht zijn voor een kleine organisatie en binnen het bereik van de organisatie komen om toegepast te kunnen worden in de mechanismen en procedures. > Voorzien in de andere verplichtingen wordt veelal ingevuld door leveranciers met een voldoende omvang. Afhankelijk van de aard en omvang van het dienstenpallet wordt invulling gegeven aan passende technische en organisatorische maatregelen. > Het bestuurlijk gesprek zal ook gaan over het adequaat voorzien in de verplichtingen. Uitgangspunt is invulling te geven aan "accountability" opdat de accountant belast met het samenstellen van de jaarrekening zijn werk kan doen.	documentatie van de verzoeken worden vastgelegd. De FG wordt hierbij steeds geïnformeerd, ziet toe op het afgesproken proces en maakt steeds de afweging in hoeverre secundaire overwegingen aan de verzoeken ten grondslag liggen. > De FG houdt de formele actualiteiten bij en gaat na welke maatregelen binnen bereik van de organisatie komen om toegepast te kunnen worden in de mechanismen en procedures. Natuurlijke momenten zijn het vervangen van informatiesystemen en het opnieuw aangaan van dienstverleningsovereenkomsten. > Het voorzien in de andere verplichtingen worden vanuit de eigen organisatie geïnitieerd. De interne controle gericht op het effectief vaststellen van de werking beheers- en beveiligingsmaatregelen vindt systematisch plaats. Rapportage is periodiek en gericht aan de leiding. Er wordt aantoonbaar opvolging gegeven aan eventuele omissies. > Het bestuurlijk gesprek zal ook gaan over het adequaat kunnen faciliteren van deze verplichtingen en welke eventueel aanvullende maatregelen nodig zijn. Het bestuurlijk gesprek is een sluitstuk om aan te tonen dan de leiding van de organisatie "accountable" is voor het gevoerde beleid. Voor de	het kunnen vervullen van de rechten van betrokkene. Er wordt regelmatig getoetst dat de afspraken (kunnen) worden nagekomen. > De FG ziet toe op het hanteren van de afgesproken "vernietigingstermijnen" van verwerkingen. De privacycontactpersonen van de entiteiten zullen de verzoeken in behandeling nemen, zorgen dat de wettelijke termijnen worden gehaald en dat de noodzakelijke documentatie van de verzoeken worden vastgelegd. De FG wordt hierbij steeds geïnformeerd, ziet toe op het afgesproken proces en maakt steeds de afweging in hoeverre secundaire overwegingen aan de verzoeken ten grondslag liggen. Dit geldt ook voor alle andere vereisten die voortvloeien uit de wet. > De FG (en ook de contactpersonen) houdt de formele actualiteiten bij, gaat na welke maatregelen binnen bereik van de organisatie komen om toegepast te kunnen worden in de mechanismen en procedures en informeert de leiding van de entiteiten. Op basis van deze informatie zullen de entiteiten hun beleid aanpassen, plannen maken en noodzakelijke investeringen vrijmaken. Voor elk proces waar profiling wordt toegepast wordt een PIA uitgevoerd en de resultaten beoordeeld. In systeemontwikkelingstrajecten (incl. het aanschaffen van standaard pakketten en diensten) wordt de eis van PbD * 2 opgenomen in de functionele specificaties. > Het voor de legal entity faciliteren van de rechten van

[12] Een Inline-TTP wordt geplaatst binnen een procesgang en vervult de rol van notaris (tijdstempelen) of makelaar (partijen samenbrengen).

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
			accountant belast met de controle van de jaarrekening zal dit een indicatie zijn dat de organisatie "auditable" is. Uitkomsten van het bestuurlijk overleg worden openbaar gemaakt.	betrokkene is een functie van "binding corporate rules", (BCR's). > Het bestuurlijk gesprek staat in het teken van het bevestigen van de "accountability" over de werking van de effectiviteit van de getroffen beheersmaatregelen door de leiding van de organisatie. De benadering voor het bestuurlijk overleg alsmede het verslag van bevindingen worden transparant gemaakt. Hiermee is de organisatie transparant en wordt de accountant belast met de wettelijke controle gefaciliteerd de opdracht te (mogen) accepteren.

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
5. **Eerlijke verwerking**	Uitgaande van het adequaat kunnen faciliteren van de rechten van de betrokkene en voldoen van de overige verplichtingen dient de verantwoordelijke / bewerker in te staan voor een eerlijke verwerking van per-	De De administratieve organisatie en de ondersteunende informatiesystemen van de verantwoordelijke en bewerker worden uitgebouwd naar het aantoonbaar eerlijke kunnen verwerken van persoonsgegevens. De betrokkene en de verwerking van persoonsgegevens staan centraal. Er vindt geen verwerking van persoonsgegevens plaats zonder grondslag. De verantwoordelijke en bewerker zijn transparant naar de betrokkene over de verwerking van zijn of haar persoonsgegevens. De gegevens, systemen en processen zijn toegerust op een veilige, adequate en eerlijke gegevensverwerking. In de keten zijn tussen verantwoordelijken en bewerkers afspraken gemaakt over te hanteren semantiek en mores. In bewerkersovereenkomst (en, in het geval van een TTP-gedreven bewerkersovereenkomst, de TTP policy) worden de formele afspraken neergelegd. Maatregelen van interne controle zien er op dat de afspraken ook daadwerkelijk worden nagekomen. Verantwoording wordt afgelegd over de mate waarin de ketenpartners hierin slagen. Dit vereist onderhoud en voortdurende verbetering van systemen en processen en veronderstelt een zorgvuldig proces van documentatie van systemen en systeemwijzigingen. Op dit niveau is de administratieve organisatie ten aanzien van de informatieplicht naar betrokkene volledig ingeregeld en is de organisatie te allen tijde voorbereid op vragen en verzoeken van de betrokkene. Het voorbereiden en het inregelen van een proces van “continuous monitoring” kan hieraan ondersteuning geven. Op dit niveau worden eveneens serieuze stappen gezet naar een robuuste systeemarchitectuur, die voldoet aan de PbD * 2 principes. De systemen worden vernieuwd en ingericht volgens het principe van “attribute based credentials for trust” waarbij gebruik wordt gemaakt van “sticky policy”, zodat een eerlijke verwerking in stand gehouden wordt en te allen tijde voorzien wordt in de informatieplicht naar de betrokkene.		

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
	soonsgegevens met de betrokkene (klant, medewerker, patiënt of individu). Anders gezegd: er moet een grondslag zijn voor de verwerking van persoonsgegevens. De betrokkene is "in control" over zijn / haar persoonsgegevens. De verantwoordelijke / bewerker heeft de noodzakelijke voorwaarden voor een eerlijke verwerking gecreëerd en houdt die ook in stand.	> Op basis van de documentatie van de verwerkingen wordt per verwerking nagegaan in hoeverre er voor de betrokkene een eerlijke verwerking plaatsvindt. > Er wordt hierbij van uitgegaan dat de compliance informatie, de "evidence" van de effectieve werking van de maatregelen en mechanismen steeds is gedocumenteerd. De uitkomsten van de assessment vormen de basis voor de informatie die aan de betrokkene wordt overlegd. > Voor de kritische verwerkingen wordt bewijs vastgelegd van het informeren van de betrokkene. Hierbij is het belangrijk de identiteit van de betrokkene, de informatie-set en de eventuele toestemming vast te leggen. > In het bestuurlijk gesprek wordt aandacht gegeven aan het vervullen van de informatieplicht.	> De actuele documentatie van de verwerkingen vormt de basis voor het vervullen van de informatieplicht: bewerkstellingen van een eerlijke verwerking. Bij elke dialoog met een betrokkene moet worden nagegaan in hoeverre de informatieplicht adequaat is ingevuld. Het kunnen aantonen door de verantwoordelijke / bewerker dat voorzien is in deze plicht vraagt om het instellen van additionele functionaliteit in de dialoog met de betrokkene over bijvoorbeeld: is er sprake van doelbinding? is er een grondslag? en begrijpt de betrokkene de verstrekte informatie? > Als de betrokkene adequaat geïnformeerd is dan moet dat bewijs worden vastgelegd om eventueel later gebruikt te worden. Het kan nuttig zijn dat een TTP een rol vervult bij deze verplichting. Instemmingen van de betrokkene kunnen worden "afgestempeld" of in bewaring worden genomen door een inline-TTP. De verleende instemming door een betrokkene op de systemen van een bewerker, moeten toegankelijk zijn voor de verantwoordelijke(n). TTP stelt hiervoor taxonomieën beschikbaar. > Afhankelijk de aard en omvang van de verwerking van persoonsgegevens wordt gebruik gemaakt van een informatie-ecosysteem. In dit eco-systeem wordt de betrokkene "in control" gebracht over zijn of haar persoonsgegevens, is er sprake van een	> De verplichting voor een verantwoordelijke / bewerker om een eerlijke verwerking tot stand te brengen ten behoeve van de betrokkene is moeilijker in te vullen naarmate er meer en meer entiteiten en verbonden partijen tot de corporate family horen en logischerwijs ook sprake is van (zeer) veel verwerkingen van persoonsgegevens. Door de betrokkene controle terug te geven over de eigen persoonsgegevens is dit een gevolg van de wet- en regelgeving. Het kunnen beschikken over en verwerken van persoonsgegevens vormt voor de verantwoordelijke / bewerker een verantwoordelijkheid en aansprakelijkheid. Het organiseren van een eerlijke verwerking van persoonsgegevens kan het aansprakelijkheids- en kostenrisico beperken. > Een eerlijke verwerking van persoonsgegevens start met het centraal zetten van de betrokkene. Het organiseren van een informatie-ecosysteem – al dan niet onder gezag van een TTP – waarin een wederkerige relatie met een betrokkene mogelijk is vormt de concrete uitwerking. De te gebruiken "sticky policies" komen tot stand op basis van "policy mapping" van policies van de betrokkene en de verantwoordelijke. Het ecosysteem zorgt ervoor dat de afgesproken policies worden nagekomen. Het ligt in de lijn van de verwachting dat betrokkenen gebruik zullen maken van verschillende informatie-ecosystemen. Vanuit het oogpunt van interoperabiliteit zullen de policies taxonomiegedreven zijn. > De verantwoordelijke richt een eerlijke verwerking voor de betrokkene in en wil graag bevestiging van de betrokkene

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
			"sticky policies" en kan de betrokkene deze policies beheren. > Overwegingen van de organisatie voor een bepaalde typologie van verwerken van persoonsgegevens wordt gedocumenteerd en beheerd. Kan desgewenst worden overlegd aan betrokkene en toezichthouder. Centraal staat de argumentatie van het voeren van een eerlijke verwerking met een betrokkene. > Het bestuurlijk gesprek zal gaan over de mate waarin de organisatie slaagt een eerlijke verwerking te faciliteren.	dat het ook als een eerlijke verwerking wordt ervaren (de bevestiging verlaagt immers het aansprakelijkheidsrisico). In navolging van het faciliteren van de rechten van betrokkene zal het proces taxonomiegedreven zijn. De TTP voorziet desgewenst in de taxonomieën. De functie van TTP kan worden uitgebreid met een inline-TTP voor het borgen van het bewijs. > Het organiseren van een eerlijke verwerking binnen de grenzen van de legal entity kunnen wij zien als een functie "binding corporate rules", (BCR's). > De vraag in hoeverre dat er sprake is van een eerlijke verwerking kan in opzet worden beantwoord door na te gaan op welke wijze het beleid is gerealiseerd. Het vaststellen van de effectieve werking van getroffen maatregelen is moeilijke vast te stellen. Uitgaande van de gedocumenteerde verwerkingen wordt nagegaan op welke wijze processen gereed zijn gemaakt en hoe het informeren van de betrokkene heeft plaatsgevonden. > In het bestuurlijk gesprek wordt nagegaan in hoeverre er aanleiding of noodzaak bestaat bestaande informatiearchitecturen te verlaten en nieuwe toe te passen. De rechten van de betrokkene worden afgewogen tegen de kosten voor investeringen alsmede de aansprakelijks- en kostenrisico's van de organisatie.

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
6. **Georganiseerd zijn**	Uitgaande van een eerlijke verwerking van persoonsgegevens worden toekomst bestendige stappen in de informatie-infrastructuur gezet. Gegevensbescherming en privacy zijn "ingebouwd" in de organisatie. Niet alleen in de informatiesystemen maar ook in de administratieve organisatie en handelen van medewerkers, leveranciers en klanten. Het streven is dat de organisatie PbD * 2 toe past en hiermee zijn de verwerkin-	Gegevensbescherming, privacy en informatiebeveiliging zijn geoperationaliseerd in de organisatie. Het kennisniveau in de organisatie wordt gewaarborgd door e-learning en opleidingen, de principes van PbD * 2 zijn leidend in de opzet en aanpassingen van informatiesystemen. Op dit niveau ligt de nadruk op het verder inregelen van de administratieve organisatie en adequaat crisis-, risico- en compliance management. Dit betekent dat een organisatie op dit niveau de privacy en security accounting en ondersteunende administratie zo heeft ingericht dat men op basis van bewijsvoering (evidence) de effectieve werking van de beheers- en beveiligingsmaatregelen kan aantonen. De organisatie heeft daartoe technieken van continuous monitoring in de administratieve systemen opgenomen. Het verantwoordingsproces is zodanig ingericht dat de leiding kan aantonen, dat de organisatie aan de verplichtingen van de wet- en regelgevingen, neergelegd in een normenkader kan voldoen. Het proces van verantwoording veronderstelt dat het leiding een privacy en security paragraaf heeft opgenomen in het jaarverslag en zich kan verantwoorden over het gevoerde privacy en security-beleid. De systemen en maatregelen en procedures worden regelmatig verbeterd en getoetst, en er worden stappen gezet om de continuïteit van de privacy en security gerelateerde maatregelen te waarborgen. Op dit niveau is het mogelijk en zinvol om een audit te laten uitvoeren, opdat het bestuur kan aantonen 'in control' te zijn voor wat betreft de opzet, het bestaan en de werking van de gegevensbescherming, privacy en informatiebeveiliging		
		> Een kleine organisatie is adequaat georganiseerd als redelijkerwijs (en dat is een inspanningsverplichting) voor de verwerkingen van persoonsgegevens aan de verplichtingen van gegevensbescherming, privacy en informatiebeveiliging is voldaan. > Kennis van zaken van wat de betrokkene van de organisatie / bewerker mag verwachten vormt een belangrijk uitgangspunt voor het treffen van passende beheer- en beveiligingsmaatregelen. Hierdoor wordt de juiste keuze gemaakt voor	> Georganiseerd zijn voor gegevensbescherming, privacy en informatiebescherming is een resultaatverplichting. Aansprakelijkheids- en kostenrisico's moeten beperkt worden tot het niveau wat de leiding aangeeft. Bewijs van adequate werking van maatregelen en mechanismen zijn op enig moment voor handen. En dat geldt ook voor het adequaat afwerken van incidenten / datalekken. Vragen van toezichthouders, raden van commissarissen / toezicht en interne of externe accountants moeten adequaat beantwoord kunnen worden. > Bewustzijn; In de organisatie zelf zijn maatregelen nodig om de medewerkers aantoonbaar bewust te maken van gegevensbescherming en privacy en de eigen verantwoordelijkheid van de medewerker Het gaat dan om het onderkennen van incidenten / datalekken en daarop adequaat reageren.	> Voor grote organisaties vormt het voldoen aan de wet- en regelgeving op het vlak van gegevensbescherming, privacy en security een resultaatverplichting. Deze resultaatverplichting geldt in een open netwerk van entiteiten en verbonden partijen. Bewijs van adequate werking van maatregelen en mechanismen zijn op enig moment voor handen. En dat geldt ook voor het adequaat afhandelen van incidenten / datalekken. > Indien gewenst kan de organisatie aansluiten bij een TTP en gebruik maken van diens policy framework, normenkader en baseline. Het gegevensbeschermingsbeleid wordt zodoende organisatie breed verankerd. Dit geldt ook voor de te hanteren taxonomieën en mores. Zoals eerder is aangegeven vormen deze stukken belangrijke bouwstenen voor de Binding Corporate

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
	gen van persoonsgegevens inherent "compliant". De FG (in welke vorm dan ook) zorgt er voor dat de organisatie in het netwerk "accountable" is. Hiermee ligt de basis voor de toezichthouder, raad van commissarissen / toezicht en interne of externe auditor in de reguliere risicomanagement cyclus te opereren (waaronder de controle van de jaarrekening).	het toepassen van geïntegreerde en afdoende maatregelen, die het opleggen van een sanctie van materieel belang tot een aanvaardbaar niveau weet te verlagen en het restrisico kan worden verzekerd. > De mix van maatregelen moet effectief zijn en natuurlijk ook efficient. Het "kunnen laten zien" dat de organisatie "accountable" (georganiseerd) is vormt een aandachtspunt. > In het bestuurlijk gesprek wordt aandacht gegeven aan een adequate mix van maatregelen en besproken op welke wijze het maatschappelijk verkeer bediend kan worden.	De FG beoordeelt de samenhang en stelt passende maatregelen voor. In een netwerk opereert de organisatie en ook de FG niet solitair. Wanneer een TTP de samenwerking modereert, kan de FG beter inspelen op actualiteiten en incidenten. Dit met als doel kennis op te bouwen en de-escalerend op te treden. > De keuze voor het inrichten van de administratieve organisatie en deze laten ondersteunen door informatiesystemen is cruciaal voor het kunnen aantonen van de effectieve werking van de maatregelen en mechanismen. Onvolkomenheden zullen uiteindelijk met additionele maatregelen "gerepareerd" worden. Hiermee wordt de beheersorganisatie complexer en (veelal veel) duurder dan nodig. PbD * 2 kunnen wij goed vertalen naar technieken van "continuous monitoring / auditing". Maatregelen kunnen worden getroffen in de technische infrastructuur. Wij denken hierbij niet alleen aan bedreigingen van buiten af maar ook van binnen uit. Op het vlak van het afrollen van verwerkingen / processen kunnen technieken van procesmonitoring worden toegepast. Het verzamelde bewijs van adequaat functioneren (in een netwerk) vormt de basis voor de "accountability" van de organisatie. > In het bestuurlijk gesprek staat de "accountability" centraal. Hiervan afgeleid de effectieve werking van de beheers- en beveiligingsmaatregelen alsmede suggesties voor een meer effectievere en meer efficiëntere mix van maatregelen.	Rules, BCR. > In de sfeer van de maatregelen ligt het voor de hand dat de organisaties zelf bepalen welke beheers- en beveiligingsmaatregelen effectief zullen zijn. Op basis van technieken van "continuous monitoring / auditing" wordt door het compliance cluster de werking van de maatregelen vastgesteld. Om georganiseerd te zijn, kan het kan noodzakelijk zijn dat een organisatie de controle over de persoonsgegevens overdraagt aan de betrokkene. Dit kan ook zijn doordat de organisatie wordt gedwongen een dergelijke stap te zetten. Hiermee wordt de keten omgedraaid en ontstaat er een zogenaamd informatie-ecosysteem. Met het omdraaien van de keten ontstaan nieuwe business modellen en markten. Vanuit het oogpunt van continuïteit van de bedrijfsvoering is het belangrijk dat de organisatie tijdig inspeelt op deze ontwikkelingen en haar bakens verzet. > In het bestuurlijk gesprek staat de "accountability" van de organisatie centraal. Hiervan afgeleid de effectieve werking van de beheers- en beveiligingsmaatregelen alsmede suggesties voor een meer effectievere en meer efficiëntere mix van maatregelen.

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
7. **Behoorlijk bestuur**	Er is sprake van een heldere besluitvormingsstructuur voor beleid, financiering, aanpak en realisatie voor gegevensbescherming, privacy en informatiebeveiliging als onderdeel van het in standhouden van een verantwoorde bedrijfshuishouding. De organisatie kan zich naar het maatschappelijk verkeer en daarmee naar betrokkene en andere organisaties in de keten verantwoorden en er ontstaat een samenspel van het	De administratieve organisatie voorziet in een adequate inrichting van de verantwoordingsinformatie en inrichting van een adequate verantwoordingsorganisatie en heldere besluitvorming. De administratieve organisatie voor risicomanagement, crisismanagement en compliance-management is ingericht, en de rapportagelijnen zijn helder. Het bestuur kan zich te allen tijde verantwoorden over het gevoerde privacy-beleid en interne beheers- en beveiligingsmaatregelen. Het bestuur kan zich naar het maatschappelijk verkeer verantwoorden, door een transparante rapportage. Het systeem van continuous monitoring en auditing bevestigt dat de organisatie, systemen en procedures betrouwbaar zijn en maakt dit aantoonbaar. Op dit niveau streeft de organisatie naar een continue verbetering van de maatregelen en systemen en draagt zorg voor de continuïteit en efficiency van de organisatie en besluitvorming voor wat betreft gegevensbescherming, privacy en informatiebeveiliging. Dit betekent dat het beleid regelmatig wordt getoetst en geëvalueerd. Privacy, gegevensbescherming en informatiebeveiliging vormt een onderdeel van de audit die (in het kader van de jaarrekening) wordt uitgevoerd. De werking van de computer crisis management organisatie (CERT Computer Emergency Response Team) is getoetst en het team functioneert in een netwerk van aanpalende CERTs. De organisatie is daadwerkelijk “accountable” en “auditable” op dit niveau, legt verantwoording af aan de toezichthouder en/of het maatschappelijk verkeer en is daarin transparant.		
		> De organisatie is afdoende georganiseerd als zij aan het maatschappelijk verkeer en met name de betrokkene kan aantonen “accountable” te zijn. Ten aanzien van Behoorlijk bestuur zal de kleine organisatie leunen op de maatregelen die de bewerker (een middel of grote organisatie) in de keten heeft georganiseerd. > Binnen de branche waar de kleine organisatie opereert zal een veelheid van vergelijkbare kleine organisaties gebruik maken van dezelfde bewerker in de keten. > Namens de kleine organisaties kan een geregisseerde interne audit bij de be-	> De organisatie heeft aangetoond georganiseerd te zijn, heeft continuous monitoring en auditing beschikbaar om een eventueel incident en datalek snel vast te kunnen stellen en opvolgen opdat schade geminimaliseerd wordt. Interne compliance audits geregisseerd. Een TTP kan dit faciliteren en bevestigen dat adequate governance maatregelen bestaan en de externe accountant heeft dat bevestigd in haar opdracht tot samenstellen en of controleren van de jaarrekening. > De governance structuur voorziet daarnaast in een crisis management organisatie voor het kunnen beheersen en controleren van grote incidenten op het gebied van gegevensbescherming. De gedragscode, indien van toepassing, is goedgekeurd door het CBP ex artikel 16 van de Wbp. Een bestuurder	> Het bestuur (de *verantwoordelijke*) van de organisatie en al haar dochterbedrijven/meerderheidsdeelnemingen en verbonden partijen hebben aangetoond dat zij zich conformeren aan het policy framework, normenkader en baseline van de moederorganisatie en zodoende compliant zijn met wet- en regelgeving en daarmee de rechten van de betrokkenen volledig respecteren. Continuous monitoring en auditing zijn beschikbaar om een eventueel datalek snel vast te kunnen stellen en op te volgen opdat schade geminimaliseerd wordt. Interne compliance audits geregisseerd in overleg met een TTP bevestigen het adequate governance maatregelen en de externe accountant heeft dat bevestigd in haar opdracht tot samenstellen en of controleren van de jaarrekening. > De governance structuur voorziet in een crisis management organisatie voor het kunnen beheersen en controleren van grote incidenten op het gebied van gegevensbescherming. De

Bijlage: Maturity levels

Level	Omschrijving	Klein	Middel	Groot
	over en weer elkaar decharge verlenen. De keten is transparant naar de toezichthouder en incidenten als zij zich toch voordoen zijn altijd onder controle.	werker en de door de externe auditor van die bewerker beoordeelde uitkomst daarvan plaatsvinden. De decharge bij alle kleine organisaties kan gefaciliteerd worden door een TTP. Het Privacy Seal bevestigt, ondersteunt door de Privacy Seal policy dat aan de eis van Behoorlijk Bestuur door de kleine organisatie is voldaan. > In het bestuurlijk gesprek bepaalt de continuïteit en het verder bereiken van efficiency in het op peil houden van Behoorlijk bestuur vanaf nu de agenda.	is aangewezen als portefeuillehouder voor privacy en gegevensbescherming. Gegevensbescherming is een vast onderwerp in het Audit Commitee van de Raad van Commissarissen / Toezicht indien beschikbaar, anders van het Dagelijks Bestuur (RvB). Er is sprake van continu toetsen van het privacy beleid en opvolging beveiligings-incidenten. > De klantengroep (verantwoordelijken) kleine organisaties heeft onder orkestratie van een TTP *'en group'* decharge verleend aan de uitvoering van de bewerkersovereenkomst. Het Privacy Seal laat dit ook zien. Daar waar onzekerheden zijn blijven bestaan en in overleg met een TTP kan het Audit Committee of indien niet aanwezig de verantwoordelijke tot aanvullende Compliance- en IT-audits opdracht geven. > In het bestuurlijk gesprek zal het continueren van Behoorlijk bestuur, het efficiënter maken daarvan en het opvolgen van ontwikkelingen vanuit het maatschappelijk verkeer onderwerp van discussie blijven.	gedragscode, indien van toepassing, is goedgekeurd door het Cbp ex artikel 16 van de Wbp. Een bestuurder is aangewezen als portefeuillehouder voor privacy en gegevensbescherming. Gegevensbescherming is vast onderwerp in het Audit Commitee van de Raad van Commissarissen / Toezicht. Er is sprake van het continu toetsen van het privacy beleid en de opvolging van beveiligingsincidenten. De getroffen maatregelen zijn vastgelegd. De verantwoordelijke in het Dagelijks Bestuur (RvB) kan worden bevraagd en ter verantwoording worden geroepen. Dit alles is aantoonbaar via verslaglegging. > De klantengroep (verantwoordelijken) kleine organisaties heeft onder orkestratie van een TTP *'en group'* decharge verleend aan de uitvoering van de bewerkersovereenkomst. Ook middel grote klantenorganisaties hebben onder regie van een TTP decharge verleend. Het Privacy Seal laat dit ook zien. Daar waar onzekerheden zijn blijven bestaan en in overleg met een TTP kan het Audit Committee tot aanvullende Compliance- en IT-audits opdracht geven. > In het bestuurlijk gesprek zal het continueren van Behoorlijk Bestuur, het efficiënter maken daarvan en het opvolgen van ontwikkelingen vanuit het maatschappelijk verkeer onderwerp van discussie blijven