Factsheet
Organiseren van de Verantwoordingsverplichting

"Verantwoordelijk zijn voor compliance met wettelijke en contractuele verplichtingen"

220202

Wat is de verantwoordingsplicht?

Diverse wetten kennen een verantwoordingsplicht. Het bekendste voorbeeld is de Belastingwet. De Europese Algemene verordening gegevensbescherming (AVG) is een ander voorbeeld. Om aan de wettelijke verantwoordingsplicht van deze wet te voldoen, is het nodig dat bedrijven en personen zich tijdig verantwoorden met betrouwbare gegevens aan de toezichthouders.

Maar bedrijven hebben ook een verantwoordingsplicht naar elkaar, zeker als deze bedrijven in een keten met elkaar verbonden zijn en persoonsgegevens uitwisselen.

Ook wensen personen die hun gegevens met bedrijven willen delen, zekerheid dat op een juiste wijze met hun gegevens wordt omgegaan.

MYOBI helpt bedrijven om deze verantwoording met eenzelfde methodiek naar al deze belanghebbenden te organiseren.

De toezichtsarrangementen

Wettelijke verantwoordingsplichten beïnvloeden zowel het gedrag van bedrijven en personen als die van toezichthouders. In de fiscale wetgeving leidt onjuiste verantwoordingsinformatie tot omdraaiing van de bewijslast, schattingen van belastbare bedragen en boetes.

In de AVG leidt onjuiste verantwoordingsinformatie tot aansprakelijkstellingsrisico's en boetes voor bedrijven. De omdraaiing van de bewijslast is daar al verankerd met een meldplicht datalekken. Zowel de fiscale wetgeving als de AVG gaan uit van een ketenaansprakelijkheid voor de hoofdaannemer, resp. de verwerkingsverantwoordelijke.

De verschillende onderling conflicterende toezichtsarrangementen van de wetgever veroorzaken bij bedrijven aanzienlijke administratieve lasten en onzekerheid.

Door vanuit het perspectief van bedrijfsactiviteiten de relevante wetten voor een bedrijf op basis van – '*comply or explain*' - op elkaar af te stemmen, krijgt de leiding de mogelijkheid om met slechts enkele baselines te voldoen aan de verantwoordingsplichten van de verschillende toezichtsarrangementen. Dit geeft een operationele verlichting en meer inzicht in de aansprakelijkheids- en kostenrisico's.

Toegevoegde waarde

Compliant gedrag voor bescherming van persoonsgegevens komt altijd ten goede aan het realiseren van de bedrijfsdoelstellingen. Wij zouden zelfs kunnen zeggen dat het een voorwaarde is. Dit geldt ook voor het afschermen en het maken van afspraken over het verwerken van bedrijfsgegevens, waaronder bedrijfsgeheimen en bedrijfsinformatie.

Bovendien leidt het maken van afspraken met personen over het verwerken van hun gegevens tot het legitiem verwerken van bedrijfs- én persoonsgegevens. Met deze benadering sluit het bedrijf naadloos aan bij zijn doelgroepen.

De afspraken hebben hun weerslag op de kwaliteit van de gegevens waardoor het bedrijf zijn bedrijfsprocessen effectiever kan inrichten.

Treffen van beheersmaatregelen

Door het treffen van de juiste beheersmaatregelen biedt de verantwoordingsplicht het bedrijf kansen zich beter aan te sluiten op doelgroepen en de operationele kosten te verlagen. Het bedrijf verantwoordt zich over de effectieve werking van de getroffen beheersmaatregelen aan het maatschappelijk verkeer; in het bijzonder aan zijn partners zoals medewerkers, klanten en leveranciers.

Het bedrijf spreekt met zijn partners het object van verantwoording en het verantwoordingsproces af via het vertrouwensnetwerk en met toepassing van smart contracting. Het maken van diverse bilaterale afspraken is daardoor niet meer nodig, hetgeen veel tijd en geld bespaart.

Wat is de compliance-aanpak?

MYOBI is een Trusted Third Party (TTP) die een vertrouwensnetwerk in stand houdt. Op het vertrouwensnetwerk beschikken zakelijke gebruikers over een informatie ecosysteem waarmee zij de kwaliteit van hun gegevens in stand houden en hun eigen juridische en functionele organisatiestructuren beheren. Bovendien maken zij afspraken met hun partners over het delen en verwerken van bedrijfs- en persoonsgegevens. Deze afspraken leggen zij vast in regie- en verwerkersovereenkomsten

Alle gebruikers conformeren zich aan de TTP-policy, die in de TTP-spelregels is samengevat. Over het adequaat verwerken van de gedeelde gegevens conform de spelregels leggen bedrijven als zakelijk gebruiker verantwoording af aan het maatschappelijk verkeer via het Accountability Seal Register.

Wat is het mechanisme?

MYOBI heeft op basis van algemeen geaccepteerde verantwoordingsprocessen en richtlijnen - van met name toezichthouders - een voor bedrijven zo effectief mogelijk compliance-aanpak ontworpen.

Bedrijven kunnen de aanpak gebruiken voor het afleggen van verantwoording over hun compliance met de TTP Gedragscode AVG of deze uit te breiden naar een integrale compliance met alle relevante wettelijke en contractuele verplichtingen.

Voor de compliance met de TTP Gedragscode AVG is de compliance-aanpak gericht op het voldoen aan wettelijke en contractuele verplichtingen voor gegevensbescherming en informatieveiligheid. Doordat gebruikers daarover verantwoording afleggen bieden zij ook anderen meer zekerheid over de betrouwbaarheid van bedrijfs- en persoonsgegevens. Je zou kunnen zeggen dat betrouwbare bedrijfs- en persoonsgegevens een belangrijke bijvangst zijn van het kunnen aantonen compliant te zijn met deze wetgeving. Tegelijkertijd vormen betrouwbare bedrijfs- en persoonsgegevens een belangrijk uitgangspunt voor andere verantwoordingsplichtsverplichtingen.

Het bestuur (de leiding) formuleert beleid en geeft hierin de mate aan waarin aan wettelijke en contractuele verplichtingen zal worden voldaan. Het beleid geeft aanleiding tot het treffen van passende technische en organisatorische beheersmaatregelen.

Er wordt een mechanisme voor compliance ingericht waarbij de effectieve werking van de getroffen beheersmaatregelen wordt gemeten en vastgelegd. Deze '*boekhouding'* vormt de grondslag voor de leiding om zich te verantwoorden aan het maatschappelijk verkeer.

Hoe werkt het mechanisme?

De Functionaris voor Gegevensbescherming (FG) heeft een wettelijke taak het bestuur (de leiding) over het gegevensbeschermingsbeleid te adviseren. Deze adviserende taak heeft de FG ook als het gaat om het treffen van passende en effectieve beheersmaatregelen. De FG ziet onder meer toe op het register van verwerkingen en de privacy en security boekhouding. De wetgever heeft de FG namelijk in een – niet vrijblijvende – toezichthoudende rol geplaatst.

De leiding kan het resultaat van de naleving van het beleid het beste inschatten op basis van de 'boekhouding' en dit resultaat uitdrukken in een zelfverklaring. De positie en de rol van de FG maakt het mogelijk de zelfverklaring – *al dan niet* – te bevestigen.

Op basis van de TTP-policy neemt MYOBI de zelfverklaring plus bevestiging op in het Accountability Seal Register. Hierbij voegt MYOBI de uitkomsten van haar eigen plausibiliteitsonderzoek.

Het maatschappelijk verkeer, in het bijzonder de partners van het bedrijf, ontlenen waarde aan deze verantwoording bij het verwerken van gegevens en zakendoen.

Wat zijn de verantwoordingsinstrumenten?

De compliance-aanpak maakt en houdt de verplichtingen expliciet (in handvatten waaraan voldaan moet zijn per volwassenheidsniveau). Op het vertrouwensnetwerk met samenwerkende partners is het essentieel dat de verwachtingen over het niveau van gegevensbescherming onderling eenduidig en duidelijk zijn.

Partners oefenen op het vertrouwensnetwerk regie uit over hun gegevens op basis van een onderling geaccepteerd kwaliteitsmodel, de TTP Gedragscode AVG.

MYOBI heeft de TTP Gedragscode AVG opgenomen in de Accountability Seal Policy als een interoperabele 'taal' voor het compliant zijn met wettelijke verplichtingen ter bescherming van persoonsgegevens.

De Vereniging VIE

De Vereniging VIE (Vereniging van Informatie Ecosysteem gebruikers) heeft een belangrijke rol bij de totstandkoming en het in standhouden van de TTP Gedragscode AVG. Deze gedragscode vormt een integraal onderdeel van de TTP-policy, in het bijzonder de Accountability Seal Policy.

De Vereniging overweegt de gedragscode aan de Autoriteit Persoonsgegevens (AP) voor te leggen.

Hulpmiddelen voor Verantwoording

MYOBI initieert en begeleidt; de gebruiker van het vertrouwensnetwerk doorloopt de verantwoordingscyclus die primair is gericht op het compliant zijn met de TTP Gedragscode AVG.

MYOBI reikt hulpmiddelen aan zoals:

- Een bedrijfsspecifieke leeromgeving gericht op bewustwording van medewerkers en kennisoverdracht aan sleutelfunctionarissen;
- Baselines waarin beheersdoelstellingen en beheersmaatregelen per volwassenheidsniveau zijn uitgewerkt;
- Reputatiemanagement waarmee overzicht en inzicht in de formele en functionele organsiatiestructuur van de eigen en die van partners worden verkregen; en
- De toepassing smart contracting gericht op het afsluiten van regie- en verwerkersovereenkomsten voor het verwerken van persoonsgegevens van of door partners.

Bedrijfsspecifieke leeromgeving

Als onderdeel van het registratieproces voor gebruikers van MYOBI maakt MYOBI ook een bedrijfsspecifieke leeromgeving aan op de infrastructuur van Duthler

Academy.

In samenwerking met Duthler Academy beheert MYOBI rolgedreven bewustwordings- en trainingsprogramma's voor het beheren van informatie ecosystemen.

Volwassenheidsniveaus voor verantwoording

Bij de start van de verantwoordingscyclus zorgt MYOBI voor de baselines bescherming van persoonsgegevens en informatieveiligheid. Hiermee kan een bedrijf zelf haar volwassenheidsniveau bepalen: in hoeverre voldoet het bedrijf aan de beheersdoelstellingen van de AVG.

Aan het eind van de verantwoordingsperiode – die gelijk kan lopen met de financiële verantwoordingsperiode – zijn de vastgestelde en gedocumenteerde volwassenheidsniveaus van het bedrijf de basis voor de zelfverklaring van de leiding. De leiding zet het volwassenheidsniveau uit de zelfverklaring om in een Accountability Seal en neemt deze Seal op in het Accountability Seal Register. MYOBI publiceert het register op haar website.

Rol van de FG

De FG geeft, in diens wettelijke rol van toezichthouder op de naleving van de AVG, al dan niet een bevestiging af bij de zelfverklaring. De FG publiceert de bevestiging of het afwijkend bepaalde volwassenheidsniveau in het Accountability Seal Register. Door de publicatie van het register op de website van MYOBI wordt het volwassenheidsniveau openbaar.

Plausibiliteitstoets op de zelfverklaring

MYOBI rondt vervolgens de verantwoordingscyclus af met een plausibiliteitstoets op de zelfverklaring. MYOBI neemt de uitkomst van de toets over in het Accountability Seal Register waardoor ook deze uitkomst gepubliceerd wordt op haar website.

Handreikingen

MYOBI heeft de verantwoordingscyclus uitgewerkt in een aantal handreikingen, waarmee medewerkers de baselines kunnen toepassen en gekomen kan worden tot een zelfverklaring en de FG wordt ondersteund bij de werkzaamheden voor diens bevestiging.

Controle en waarborging door boards

MYOBI heeft een structuur ingericht om het vertrouwensnetwerk te faciliteren en te controleren. MYOBI is verantwoordelijk voor het vertrouwensnetwerk en het faciliteren van de toepassingen, zoals smart contracting en smart compliance. Daarnaast is MYOBI verantwoordelijk voor de hulpmiddelen zoals de baselines en de handreikingen. Ook voert MYOBI de toets uit op de zelfverklaring met bevestiging.

MYOBI heeft twee Boards:

- Standaardisatie Board: verantwoordelijk voor het beheren en het goed gebruiken van sets van gegevensdefinities. Gebruikers van het vertrouwensnetwerk zijn met de gegevensdefinities onderling interoperabel voor het verwerken van (persoons)gegevens; *en*
- Accountability Board: verantwoordelijk voor het toezien op de naleving van de TTP Gedragscode AVG. Deze Board geeft gevraagd en ongevraagd advies over de werking van de gedragscode.

Daarnaast heeft de Vereniging VIE een toezichthoudend orgaan, genaamd Monitoring Body.

Zowel de Accountability Board van MYOBI als de Monitoring Body van Vereniging VIE hebben het recht om zelf ook een toets uit te voeren op de juistheid van het volwassenheidsniveau dat de leiding heeft afgegeven. Zij zullen steekproefsgewijs van hun recht gebruik maken. Hun uitkomst wordt ook in het Accountability Seal Register opgenomen.

Onafhankelijke vereniging

De al eerdergenoemde Vereniging VIE heeft als doel het bevorderen van de juiste toepassing van de verantwoordingsverplichting van de AVG. Dat is immers een voorwaarde voor het uitoefen van regie over persoons- en bedrijfsgegevens op een vertrouwensnetwerk. Gebruikers moeten immers kunnen vertrouwen op de kwaliteit van de gegevens van de informatie ecosystemen.

Een instrument om de kwaliteit van gegevens in stand te houden en te bevorderen is dat gebruikers verantwoording afleggen over hun mate van compliance met de AVG. De TTP Gedragscode AVG is met name bedoeld om gebruikers een kader en instrumenten aan te bieden waarmee zij invulling kunnen geven aan hun verantwoordingsverplichting.

De Vereniging VIE heeft dan ook als afgeleid doel de instandhouding en verbetering van de gedragscode alsook het bevorderen van het toepassen van de gedragscode als instrument om op uniforme en daarmee voorspelbare wijze aan de verantwoordingsplicht van de AVG te voldoen.

Hiermee geeft de vereniging mede vorm aan interoperabele compliance. Leden van de vereniging zijn:

- Bedrijven die verwerkingsverantwoordelijke of verwerker zijn van verwerkingen die bijdragen aan de instandhouding van informatie ecosystemen; *en*
- Personen wiens gegevens object zijn van die verwerkingen door bedrijven die gebruik maken van het Vertrouwensnetwerk.

Deze bedrijven en personen zijn altijd gebruiker van een TTP. Zakelijke gebruikers – geen aspirant leden - van MYOBI worden automatisch lid van de vereniging.

Wat zijn de verwachtingen?

Gegevensbescherming en informatieveiligheid zijn na de introductie van de AVG meer volwassen geworden. De AP richtte zich aanvankelijk op het geven van advies, maar laat zich nu meer zien als handhaver.

Ondanks dat de AVG al meerdere jaren van kracht is, is de implementatie van gegevensbescherming bij veel organisaties tot nu toe beperkt gebleven tot het formeel op orde krijgen van verplichtingen. Na het uitvoeren van 'het project AVG' is de aandacht verslapt en ebt de kennis weg. Er is hernieuwde aandacht voor gegevensbescherming en informatieveiligheid nodig. Zie: het beleid van de AP voor 2020 -2023.

Ook buiten de werkingssfeer van de AVG spelen op nationale en internationale niveau ontwikkelingen die bepalend zijn voor het organiseren van gegevensbescherming en informatieveiligheid. Een voorbeeld daarvan is MedMij programma, in het bijzonder het MedMij Afsprakenstelsel. Het MedMij programma richt zich op het faciliteren van personen regie uit te oefenen over hun medische gegevens.

Ook deze ontwikkelingen hebben MYOBI ertoe gebracht het vertrouwensnetwerk verder te professionaliseren. Het doel is gebruikers van het vertrouwensnetwerk vanuit hun bedrijfsactiviteiten, proactief te faciliteren bij het voldoen aan de wettelijke en contractuele verplichtingen op het vlak van gegevensbescherming en informatieveiligheid.

Door expliciet de bedrijfsactiviteiten voorop te stellen biedt MYOBI de bedrijven de randvoorwaarden beter aan te sluiten bij hun doelgroepen en bedrijfsprocessen productiever te organiseren. Er is een duidelijke businesscase om veranderingen door te voeren.

TTP Gedragscode AVG

De TTP Gedragscode AVG vormt voor MYOBI een belangrijk onderdeel van de compliance-aanpak. De gedragscode faciliteert de interoperabiliteit van compliance met wettelijke en contractuele verplichtingen tussen de gebruikers op het netwerk. Dit biedt gebruikers zekerheid over welke beheersmaatregelen getroffen moeten worden om te voldoen aan de verplichtingen van de AVG én inzicht in de aansprakelijkheids- en kostenrisico's van non-compliance met de TTP Gedragscode AVG. De vereniging is voornemens de gedragscode voor te leggen aan de AP.

Tijdlijnen

De leiding van een bedrijf is vaak gewend om op een handmatige wijze vast te stellen dat aan de AVG wordt voldaan en houdt hiervan een dossier bij. Dat geldt ook voor de FG. Het vervullen van deze verantwoordingsverplichting uit de AVG beschouwen vele leidinggevenden als een worsteling.

De inspanningen van bedrijven zullen toenemen omdat zowel bij de Europese als de nationale toezichthouder meer aandacht is voor toezichtstaken, met name het afwerken van datalekken en overige onderzoeken. Bovendien is er sprake van toenemende uitwisseling van persoonsgegevens, het outsourcen van verwerkingen en het met gegevensverwerkingen naar de cloud gaan. Hiermee neemt de druk om zich te verantwoorden toe.

Zodra een zakelijke gebruiker zich aansluit bij MYOBI maakt het complianceteam van MYOBI met de leiding afspraken over de tijdlijnen van de verantwoording.

De zakelijke gebruiker krijgt de beschikking over hulpmiddelen die het bedrijf ondersteunen bij het afleggen van verantwoording met een zelfverklaring.

De FG die gedurende het jaar heeft toegezien op de naleving van de AVG, voegt een bevestiging toe aan de zelfverklaring waarin aangegeven wordt of het volwassenheidsniveau wordt onderschreven of dat de FG tot een afwijkend oordeel is gekomen.

Het volwassenheidsniveau, dat zowel door de leiding wordt bepaald als door de FG, wordt omgezet in een Accountability Seal en opgenomen in het Accountability Seal Register. Dit register is voor een iedere belangstellende te raadplegen. Na uitvoering van een plausibiliteitstoets voegt MYOBI het volwassenheidsniveau dat zij heeft vastgesteld toe in het register.

Neem gerust contact op met:

Caroline Willemse AA RE RFG
Hoofd compliance-team
c.willemse@duthler.nl
+31(0) 70 362 18 07
+31(0) 6 12 11 33 88

REGISTREER