Duthler Associates
law, ICT & organisation

Factsheet

Organiseren van uw verantwoording

Organiseren van uw volwassenheidsniveau door de juiste compliance-aanpak

Het toepassen van de registratievoorwaarden op het MYOBI Vertrouwensnetwerk, in het bijzonder op het eigen informatie ecosysteem, is een voorbeeld van het organiseren van de verantwoordingsplicht voor het authentiseren van de identiteit van het bedrijf en de wettelijke vertegenwoordiger (ken uw partner). Het onder regie uitwisselen van bedrijfs- en persoonsgegevens is gericht op de verantwoordingsplicht voor het beschermen van de persoonsgegevens (effectief borgen van de rechten van betrokkenen). Voor elk van de voorbeelden is er een Europese en/of nationale toezichthouder die toeziet op het nakomen van de verantwoordingsplicht.

Verantwoording met de TTP-policy organiseren

De Accountability Seal Policy is een onderdeel van de TTP-policy van MYOBI dat het verantwoorden van de naleving van deze policy regelt. Op basis van een Accountability Seal verantwoordt de directie van een bedrijf zich aan het maatschappelijk verkeer en de overige gebruikers van het vertrouwensnetwerk in het bijzonder. Hiervoor is het nodig om compliance voor de Accountability Seal te organiseren.

Wat is de compliance aanpak?

Het is efficiënt om het voldoen aan de TTP-policy die de wettelijke verantwoordingsplicht voor het beschermen van gegevens afdekt, mee te nemen in de bestaande verantwoordingscyclus. Door de tijdlijnen voor de verantwoordingen op elkaar af te stemmen ontstaat synergie in compliancewerkzaamheden en kunnen inspanningen en kosten teruggedrongen worden. De efficiency wordt verhoogd met een integrale compliance-aanpak van al deze verplichtingen.

Ieder jaar de juiste verantwoording

Om aan het eind van een jaar verantwoording te kunnen afleggen over het gehele jaar moeten gedurende het jaar voldoende compliancewerkzaamheden uitgevoerd worden. Tussentijdse uitkomsten van verantwoordingen kunnen aanleiding zijn tot bijsturing. Uitgaande van een kalenderjaar als verantwoordingsperiode wordt in het eerste kwartaal van het nieuwe jaar opgesteld over het voorgaande jaar:

- de zelfverklaring van de directie; *en*
- de bevestiging van de zelfverklaring door de functionaris voor gegevensbescherming (FG).

De zelfverklaring bestaat uit een uitspraak door de directie over het gehaalde volwassenheidsniveau en de ambitie voor het komende jaar. Deze verklaring wordt door de FG van het bedrijf of een aangewezen FG bevestigd.

Wat is onze aanpak?

Het verantwoorden over de compliance met wettelijke (AVG en of Wbb) en contractuele eisen vraagt een doortastende aanpak. Voor het beschermen van persoonsgegevens beginnen we met het inventariseren van de bedrijfsactiviteiten, de processen die deze activiteiten ondersteunen, de risico's die voor het bedrijf en/of de betrokkenen zich kunnen voortdoen en het treffen van maatregelen die effectief werken. Zoveel als mogelijk wordt aangesloten op beschikbare (standaard) baselines die aangevuld worden met bedrijfsspecifieke maatregelen. Op basis van de risicoanalyse kan bepaald worden hoe vaak vastgesteld moet worden dat een maatregel effectief werkt. Vervolgens komt het inregelen in de organisatie van verantwoordelijken en uitvoerenden die de effectiviteit van de beheersmaatregelen conform de bepaalde periodiciteit vaststellen.

Voor het beschermen van bedrijfsgeheimen beginnen we met het doorlopen van de bedrijfsactiviteiten en daarbij te inventariseren welke bedrijfsgeheimen er zijn. We kunnen een voorzet maken voor een beleid waarin de bedrijfsleiding handvatten geeft aan medewerkers hoe met bedrijfsgeheimen om te gaan. Na een risicoanalyse worden de maatregelen ingeregeld om de bedrijfsgeheimen te beschermen en periodiek te laten vaststellen of deze maatregelen effectief werken.

Persoonsgegevens

Een bedrijf loopt aansprakelijkheids- en kostenrisico's als het niet instaat is te voldoen aan de verantwoordingsplicht. Het gaat niet alleen om boetes of claims van de toezichthouder maar ook van degenen wiens persoonsgegevens worden verwerkt. Bovendien bestaat het risico op reputatieschade als zich datalekken voordoen die niet ontdekt zijn of foutief zijn afgewerkt. Om zich te kunnen verantwoorden is het nodig dat het bedrijf het beschermen van persoonsgegevens effectief heeft georganiseerd.

Het MYOBI Vertrouwensnetwerk biedt bedrijven een praktisch verantwoordingsmechanisme. Hierbij staat centraal het door het bedrijf organiseren van compliance met wettelijke en contractuele verplichtingen, in het bijzonder de TTP-policy en daarmee ook aan de TTP Gedragscode AVG. Jaarlijks spreekt de leiding zich uit in een zelfverklaring over het nakomen van deze gedragscode, uitgedrukt in een volwassenheidsniveau. Het volwassenheidsniveau wordt op de website van MYOBI gepubliceerd.

Het verantwoordingsmechanisme is op de kennisbank uitgelegd. Zie verantwoordingsplicht en verantwoorden. Wij zorgen in opdracht van MYOBI de interne controle van het verantwoordingsmechanisme.

Het belang voor partners verantwoording af te leggen over compliant zijn met de eisen van de AVG en Wbb is duidelijk; het organiseren van de compliance vraagt de nodige aandacht van de bedrijfsleiding, management en medewerkers. Een goed gesprek kan toereikend zijn ongewisheid weg te nemen.

Bedrijfsgeheimen

Een belangrijke voorwaarde om aanspraak te kunnen maken op een inbreuk op een bedrijfsgeheim, is dat het geheim goed beveiligd moet zijn. Een geheim dat niet goed beveiligd is, kan door een rechter worden bestempeld als 'niet-geheim' omdat het bedrijf niet de nodige effectieve maatregelen heeft getroffen om het geheim te houden.

Het organiseren van het beschermen van bedrijfsgeheimen is voorwaardelijk om bedrijfsgeheimen effectief te beschermen en – bij inbreuk – recht te halen onder de Wbb. Dit houdt in dat een bedrijf moet bepalen wat haar bedrijfsgeheimen zijn en welke maatregelen getroffen moeten worden om het geheim te beschermen. Vervolgens dient ingeregeld te worden dat aantoonbaar kan worden gemaakt dat de maatregelen effectief hebben gewerkt.

Een belangrijke maatregel is het afsluiten van een geheimhoudingsovereenkomst met partners die toegang tot bedrijfsgeheimen nodig hebben voor het uitvoeren van bijvoorbeeld een (uitbestedings)opdracht. Deze partners dienen zich regelmatig te verantwoorden over het nakomen van de afspraken die in deze overeenkomst zijn gemaakt. Dergelijke verantwoordingen zijn onderdeel van de eigen verantwoording van het bedrijf.

Het komt veelvuldig voor dat partners afspreken zich onderling te verantwoorden over het vertrouwelijk gebruikmaken van elkaars bedrijfsgeheimen.

Meer informatie

Neem gerust contact met ons op via +31 (0) 70 392 22 09 of info@duthler.nl. Maak een afspraak met drs. André J. Biesheuvel RA RE RFG, de service-eigenaar gegevensbescherming, of een professional van zijn team.

Duthler Associates
law, ICT & organisation

Afspraak maken en contact

Wilt u meer weten? Neem dan contact op met ons op via de onderstaande gegevens. Of bezoek onze website: www.duthler.nl

Kantoor:

Frankenslag 137

2582 HH Den Haag

+31 (0) 70 392 22 09

info@duthler.nl