Consultatie Principes voor Informatiebeveiliging

Feedbackstatement

Publicatiedatum: 19-dec-2019
Classificatie: AFM - Publiek

Autoriteit Financiële Markten

De AFM maakt zich sterk voor eerlijke en transparante financiële markten.

Als onafhankelijke gedragstoezichthouder dragen wij bij aan duurzaam financieel welzijn in Nederland.

Inhoudsopgave

1. Inleiding

Op 14 mei heeft de Autoriteit Financiële Markten (AFM) haar Principes voor Informatiebeveiliging (hierna: de principes) geconsulteerd. Deze consultatieperiode duurde tot en met 25 juni 2019. De AFM heeft van 26 organisaties opmerkingen en aanbevelingen ontvangen, waaronder accountantsorganisaties, brancheverenigingen, financiële instellingen, een Trusted Third Party, een adviesorganisatie en de beroepsgroep voor IT-auditorsprincipes. Deze reacties stellen ons in staat de (toelichting op de) principes duidelijker te maken. Wij willen hen hiervoor dan ook hartelijk danken.

De reacties op de consultatie hebben geleid tot tekstuele verbeteringen in de principes, zoals opgenomen in de definitieve versie. Daarnaast behandelen wij in dit feedbackstatement drie onderwerpen waarop in verschillende reacties om meer verduidelijking is gevraagd.

Dit betreft:
1. Wettelijk kader;
2. Proportionaliteit;
3. (Inter)nationale convergentie.

Per onderwerp geven we een korte beschrijving van de ontvangen reactie(s), waarna we de reactie(s) beantwoorden en uitleggen waarom we een bepaalde keuze maken.

2. Wettelijk kader

In verschillende reacties op de geconsulteerde principes worden vragen gesteld over hoe de principes zich verhouden tot wetgeving die toeziet op beheerste en integere bedrijfsvoering. Daarnaast is meerdere keren gevraagd om een toelichting op de verhouding tussen de principes en de Algemene Verordening Gegevensbescherming.

Wetgeving ten aanzien van bedrijfsvoering

In de inleiding van de principes is toegelicht dat principes geen nieuwe regels vormen, maar algemene uitgangspunten bevatten over informatiebeveiliging waar verschillende wettelijke normen onder liggen waarop de AFM toezicht houdt. Deze wettelijke eisen ten aanzien van de bedrijfsvoering van ondernemingen zijn bijvoorbeeld onderdeel van de Wft, MiFID, Wta en Europese verordeningen. De principes vervangen die vereisten niet. De principes bieden handvatten bij de invulling van wettelijke vereisten waarvoor de AFM dit van toegevoegde waarde acht.

Algemene Verordening Gegevensbescherming (AVG)

In Nederland is de Autoriteit Persoonsgegevens de aangewezen gegevensbeschermingsautoriteit die onafhankelijk toezicht houdt op het verwerken van persoonsgegevens. De Principes voor Informatiebeveiliging hebben als doel dat ondernemingen maatregelen treffen om de beschikbaarheid, integriteit en vertrouwelijkheid van processen, systemen, data en informatie te waarborgen. Het naleven van de principes kan bijdragen aan het nakomen van andere vereisten waar de AFM niet op toeziet, zoals de AVG. Ondernemingen moeten zelf alert zijn op de invulling hiervan.

3. Proportionaliteit

Uit de reacties op de consultatie blijkt dat er behoefte bestaat aan meer informatie over de verwachtingen van de AFM ten aanzien van proportionaliteit in de toepassing van de principes.

De AFM onderkent dat de uitvoering van de principes per onderneming zal verschillen, als gevolg van de aard van de dienstverlening en de omvang van de onderneming. De AFM wil met de Principes voor Informatiebeveiliging geen verwachtingen introduceren ten aanzien van maatregelen op het gebied van informatiebeveiliging, die ongeacht de aard en het type onderneming dienen te worden toegepast. De AFM verwacht van ondernemingen dat zij de aard van de dienstverlening en de omvang van de onderneming meewegen bij de analyse van dreigingen en risico's en de toepassing en nadere invulling van de principes in lijn is met de voor de onderneming relevante dreigingen en risico's.

Ook van kleine partijen verwacht de AFM dat zij de principes vertalen naar hun organisatie. In de praktijk kan dit leiden tot minder vergaande informatiebeveiligingsmaatregelen dan middelgrote en grote organisaties.

4. (Inter)nationale convergentie

Verschillende ondernemingen merken op dat er overlap lijkt te bestaan tussen de geconsulteerde Principes voor Informatiebeveiliging en het toezicht van De Nederlandsche Bank (DNB) op informatiebeveiliging. Zij vragen zich af wat de toegevoegde waarde is van de publicatie van de principes in aanvulling op de door DNB gepubliceerde Good Practice Informatiebeveiliging.

Daarnaast is de vraag gesteld hoe de principes zich verhouden tot internationale regels en richtlijnen.

Nationale convergentie

Het toezicht op de beheerste en integere bedrijfsvoering van ondernemingen wordt primair gevoerd door de vergunningverlenende toezichthouder (primaire toezichthouder). De ondernemingen in scope van de Principes voor Informatiebeveiliging zijn opgenomen in bijlage 1. Dit betreft ook bepaalde ondernemingen waar DNB prudentieel toezicht op voert. Waar nodig vindt afstemming plaats om consistentie te waarborgen en waar nuttig zal de AFM gebruik maken van de Good Practice Informatiebeveiliging 2019-2020 van De Nederlandsche Bank.

Internationale convergentie

De AFM is voorstander van Europese en internationale convergentie om het toezicht op informatiebeveiliging en cybersecurity te harmoniseren. In ESMA verband zet de AFM zich in om tot deze harmonisatie te komen. Wanneer een onderneming een van de internationaal erkende raamwerken voor informatiebeveiliging toepast, voldoet zij in beginsel aan de verwachtingen die de AFM heeft op het gebied van informatiebeveiliging. Dit is expliciet in de principes opgenomen.

Autoriteit Financiële Markten
T 020 797 2000 | F 020 797 3800
Postbus 11723 | 1001 GS Amsterdam
www.afm.nl