Uitvraag uitbesteding

Handleiding

Mei 2020

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.

Waarom vraagt de AFM naar uitbesteding?

Uitbesteding van activiteiten vraagt om een adequate beheersing van de risico's die volgen uit uitbesteding door financiële ondernemingen. Zeker als het gaat om uitbesteding van activiteiten binnen primaire processen van financiële ondernemingen. De AFM heeft uw antwoorden nodig om inzicht te krijgen in welke risico's, waar en in welke mate bij ondernemingen voorkomen en de mate waarin en wijze waarop deze risico's worden beheerst. Met dit inzicht kan de AFM zorg dragen voor proactief en risicogestuurd toezicht op uitbesteding.

Naar welke activiteiten vraagt de AFM in deze uitvraag?

De AFM hanteert voor uitbesteding de definitie van uitbesteden zoals opgenomen in artikel 1:1 van de Wet op het financieel toezicht:

'*het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden:*

a. die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten; of

b. die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan;'

U moet alle belangrijke of kritieke activiteiten melden die uw onderneming heeft uitbesteed, aan externe partijen of intragroep. Het gaat hierbij om activiteiten die betrekking hebben op het primaire proces van uw onderneming.

Wat is een belangrijke of kritieke uitbesteding?

U kunt als vuistregel hanteren dat uitbesteding belangrijk of kritiek is indien het tijdelijk of permanent uitvallen van de onderliggende activiteit leidt tot ongewenste juridische, operationele en/of financiële risico's voor uw onderneming en de klanten van uw onderneming.

Om te beoordelen of de activiteit die uw onderneming uitbesteedt belangrijk of kritiek is, voert u zelf een materialiteitsassessment uit. Hiervoor kunt u bijvoorbeeld de volgende criteria gebruiken:

- In hoeverre de uitbestede activiteit essentieel is voor de bedrijfscontinuïteit, bedrijfsvoering en levensvatbaarheid van uw onderneming. Hierbij kunt u de vraag stellen of het voor uw onderneming mogelijk is om aan de verplichtingen aan klanten te voldoen zonder deze activiteit;
- Het directe operationele effect van onderbrekingen van de uitbestede activiteit en de hiermee gepaard gaande juridische en operationele risico's;
- Het effect op de verwachte inkomsten van uw onderneming bij verstoring van de uitbestede activiteit;
- De gevolgen van een schending van de vertrouwelijkheid, integriteit of beschikbaarheid van de gegevens voor uw onderneming en de klanten van uw onderneming.

Over welke periode gaat de rapportageverplichting?

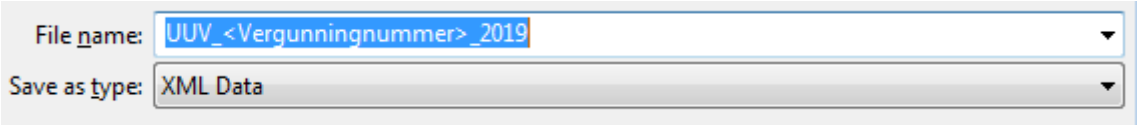
Deze rapportageverplichting gaat over het tijdvak 2019. Geef in uw beantwoording de activiteiten door die uw onderneming in 2019 uitbesteedde. Vermeld zowel de activiteiten waarvan de uitbesteding in 2019 eindigde als de activiteiten waarvan de uitbesteding na 2019 doorloopt. Uitbestedingen die na 1 januari 2020 zijn gestart hoeft u niet door te geven in deze rapportage, maar kunt u in 2021 over 2020 rapporteren.

Hoe moet het rapportagebestand worden opgeslagen?

Wanneer u gebruik maakt van het Excel Invulblad dient u met de volgende zaken rekening te houden.

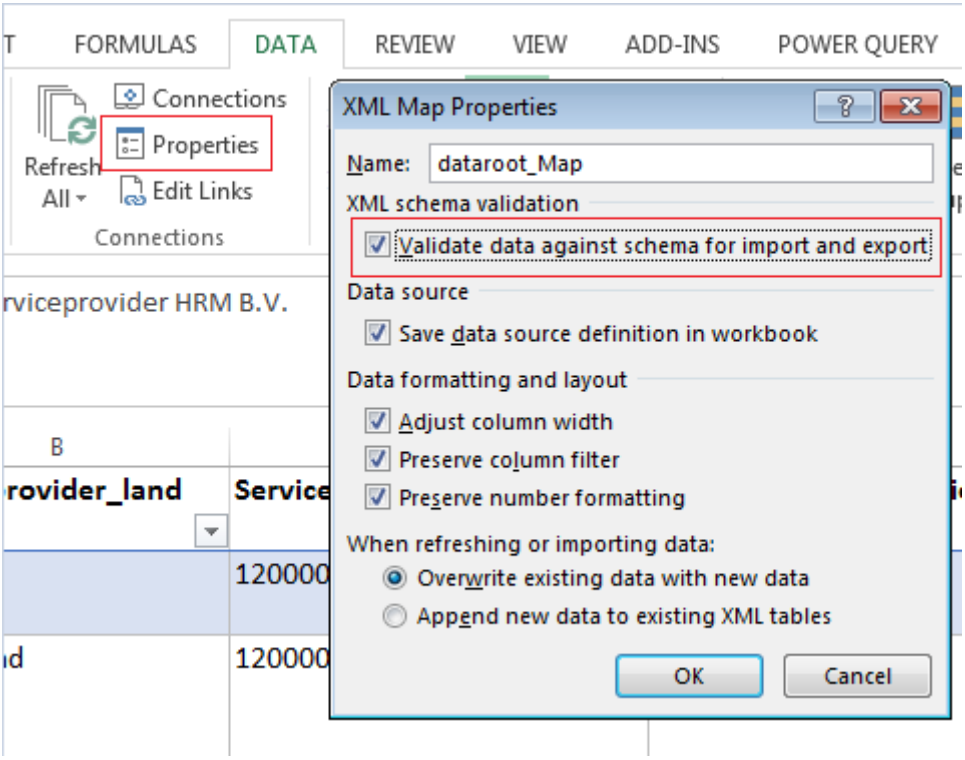
Opslaan als XML-bestand

Om de data in het Excel Invulblad als een geldig XML-bestand op te slaan dient u te kiezen voor ‘Save As / Opslaan Als’ en dan voor het type ‘XML Data’.



Validatie

Bij het opslaan als XML wordt de data automatisch gevalideerd indien de optie ‘Validate data against schema for import and export’ is aangevinkt in het menu Data / Properties:



In deze validatie wordt gecontroleerd of:

- Verplichte velden zijn ingevuld.
- Ingevulde waarden voldoen aan opgegeven waardenbereiken.
- Waarden voldoen aan overige technische vereisten.

Wanneer de data niet voldoet aan deze vereisten, verschijnt een melding in het scherm maar het bestand wordt wel opgeslagen. U dient er dan zelf voor te zorgen dat de gesignaleerde onvolkomenheden alsnog in de data worden opgelost. Dat kan door in het Excel invulblad de juiste verbeteringen door te voeren en de data opnieuw op te slaan (waardoor deze opnieuw gevalideerd wordt).

Bij het opslaan als XML Data wordt er automatisch voor gezorgd dat de juiste datatypes worden toegepast.

Wie ondertekent de rapportage bij verzending?

De rapportage moet bij de verzending ondertekend worden door een beleidsbepaler van uw onderneming. De beleidsbepaler verklaart door ondertekening dat de rapportage naar waarheid is ingevuld.

Vertrouwelijkheid

De AFM gaat zorgvuldig om met de gegevens die u aan ons doorgeeft. Het uitwisselen van gegevens met derde partijen is gebonden aan voorwaarden die bij wet zijn voorzien. Tussen de AFM en DNB is een convenant gesloten om dubbele toezichtlasten te voorkomen.

Vragen

Als u nog vragen heeft, kunt u op werkdagen van 10:00 tot 17:00 contact opnemen met het ondernemersloket. Het telefoonnummer is 0800 - 6800 680. U kunt ook het contactformulier invullen op www.afm.nl/professionals/contact.

Toelichting per vraag

De vetgedrukte begrippen worden in de lijst van definities toegelicht.

1. Wat is de naam van de **serviceprovider** waaraan de activiteit is uitbesteed?
   Vul de volledige statutaire naam in van de serviceprovider die u de uitbestede dienst levert. Deze statutaire naam kunt u op www.kvk.nl vinden als de serviceprovider in Nederland gevestigd is. Als de serviceprovider buiten Nederland is gevestigd, kunt u de statutaire naam bij de serviceprovider opvragen.

2. In welk land is de serviceprovider gevestigd?
   Vul het land in waar de hoofdvestiging van uw serviceprovider is gevestigd.

3. Wat is het KVK-nummer van de serviceprovider?
   Vul het 8-cijferige KVK-nummer van de hoofdvestiging van de serviceprovider in. **Als de serviceprovider buiten Nederland gevestigd is, laat het veld dan leeg.**

4. Is de serviceprovider een intragroup entiteit?
   Vul in of de serviceprovider onderdeel is van dezelfde groep als uw onderneming.

5. Wat zijn de totale kosten die in 2019 voor de dienstverlening in rekening zijn gebracht door de serviceprovider?
   Vul de totale kosten exclusief BTW in die de serviceprovider gedurende het tijdvak in rekening heeft gebracht bij uw onderneming. Vermeld de bedragen in euro's, afgerond op hele euro's. Gebruik hierbij geen leestekens. **Voorbeeld: als de kosten € 1.000 waren, vult u in het veld '1000' in.**

6. Wat is de startdatum van de dienstverlening door de serviceprovider?
   Vul de datum in waarop de dienstverlening van de serviceprovider begonnen is met de levering van diensten aan uw onderneming. Het gaat hierbij om de eerste dag waarop de serviceprovider uw onderneming diensten leverde, ook als dit onderdeel van een projectfase of gefaseerde migratie was. Het datumformaat is DD-MM-JJJJ. **Voorbeeld: 01-01-2019**

7. Welke dienst levert de serviceprovider uw onderneming?
   Geef een beknopte beschrijving van de soort dienstverlening die de serviceprovider aan uw onderneming levert.
8. Heeft de dienstverlening van de serviceprovider een IT-component?
   Geef aan of de serviceprovider uw onderneming als onderdeel van de uitbesteding IT-diensten levert.

9. Zijn er andere serviceproviders in de markt die dezelfde soort dienstverlening aanbieden?
   Geef aan of er andere serviceproviders in de markt zijn die uw onderneming dezelfde dienstverlening kunnen leveren.

10. Is er sprake van **gegevensverwerking** door de serviceprovider?
    Vul hier in of de serviceprovider gegevens voor uw onderneming verwerkt.

Als er uitsluitend sprake is van gegevensopslag zonder bewerking van de gegevens, vul hier dan 'nee' in.

11. In welk land worden de gegevens verwerkt?
    Vul het land in waar de gegevensverwerking plaatsvindt. In sommige gevallen vindt gegevensverwerking in meerdere landen plaats. Vul dan het land in waar de gegevens als eerst worden verwerkt door de serviceprovider.
    Vul dit veld alleen in als u bij de vorige vraag heeft gekozen voor 'Ja'. Laat het veld anders leeg.

12. Is er sprake van g**egevensopslag** door de serviceprovider?
    Vul in of de serviceprovider de gegevens (data) van uw onderneming opslaat.

13. In welk land worden de gegevens opgeslagen?
    Vul het land in waar de gegevens (data) worden opgeslagen.
    Vul dit veld alleen in als u bij de vorige vraag heeft gekozen voor 'Ja'. Laat het veld anders leeg.

14. Heeft uw onderneming een **risico analyse** uitgevoerd voorafgaand aan de uitbesteding?
    Vul in of er een formele en gedocumenteerde risico analyse door uw onderneming heeft plaatsgevonden voorafgaand aan de uitbesteding.

*De volgende drie vragen gaan over de **BIV-classificatie** van de uitbesteding. Wij vragen u om hierbij een score toe te kennen aan de uitbestede activiteit op basis van het belang van de activiteit voor uw onderneming in het tijdvak.*

15. Hoe scoort uw onderneming voor deze uitbesteding de risico's voor het aspect '**beschikbaarheid**'?
    Vul in hoe uw onderneming de risico's voor het aspect 'beschikbaarheid' scoort. Kies uit:
    1. Zeer laag
    2. Laag
    3. Midden
    4. Hoog
    5. Zeer hoog

16. Hoe scoort uw onderneming voor deze uitbesteding de risico's voor het aspect '**integriteit**'?
    Vul in hoe uw onderneming de risico's voor het aspect 'integriteit' scoort. Kies uit:
    1. Zeer laag
    2. Laag
    3. Midden
    4. Hoog
    5. Zeer hoog

17. Hoe scoort uw onderneming voor deze uitbesteding de risico's voor het aspect '**vertrouwelijkheid**'?
    Vul in hoe uw onderneming de risico's voor het aspect 'vertrouwelijkheid' scoort. Kies uit:
    1. Zeer laag
    2. Laag
    3. Midden
    4. Hoog
    5. Zeer hoog

18. Is er een ondertekend contract voor de uitbesteding?
    Vul in of de uitbesteding contractueel vastgelegd en ondertekend is door uw onderneming en de serviceprovider.

19. Wat is de reden dat er geen ondertekend contract is?
    Vul in waarom er geen ondertekend contract is voor de dienstverlening door de serviceprovider aan de onderneming waarvoor u deze uitvraag beantwoordt. **Vul dit veld alleen in als u bij de vorige vraag heeft gekozen voor 'Nee'. Laat het veld anders leeg. Als u het veld heeft gevuld met de reden waarom er geen contract is, hoeft u de rest van de vragen over deze uitbesteding (vraag 4.3-5.15) niet te beantwoorden. U kunt verder gaan met de beantwoording van de vragen voor een (eventuele) volgende uitbesteding en hiervoor weer bij vraag 1.1 beginnen.**

20. Wat is de startdatum van het contract met de serviceprovider?
    Vul de ingangsdatum in van het contract voor de levering van diensten door de serviceprovider aan uw onderneming. Het datumformaat is DD-MM-JJJJ. **Voorbeeld: 01-01-2019.**

21. Wat is de einddatum of renewal date van het contract met de serviceprovider?
    Vul de einddatum of de datum waarop het contract tussen de serviceprovider en uw onderneming moet worden vernieuwd in. Het datumformaat is DD-MM-JJJJ. **Voorbeeld: 01-01-2019**.

22. Bevat het contract een **exit clausule**?
    Vul in of er een exit clausule is opgenomen in het contract.

23. Is in het contract **auditrecht** voor uw onderneming opgenomen?
    Vul in of het recht op audit bij de serviceprovider door uw onderneming is opgenomen in het contract.

24. Is het **auditrecht** voor externe accountants en/of toezichthouders opgenomen in het contract?
    Vul in of het recht op audit bij de serviceprovider door externe accountants en toezichthouders is opgenomen in het contract.

25. Zijn er afspraken in het contract opgenomen over **onderuitbesteding** door de serviceprovider?
    Vul in of er afspraken in het contract zijn opgenomen over onderuitbesteding door de serviceprovider.

26. Is in het contract opgenomen dat de serviceprovider jaarlijks een **third party assurance type 2 verklaring** overlegt?
    Vul in of er in het contract is opgenomen dat de serviceprovider jaarlijks een third party assurance type 2 verklaring afgeeft.

27. Zijn er **performance incentives** voor de serviceprovider opgenomen in het contract?
    Vul in of er performance incentives zijn opgenomen in het contract.

28. Hoe vaak stuurt de serviceprovider een (performance-) rapportage?
    Vul in hoe vaak de serviceprovider een performance-rapportage stuurt. Kies hierbij het antwoord dat het dichtst bij de werkelijkheid aansluit.

29. Hoe vaak vinden er evaluatiegesprekken plaats met de serviceprovider?
    Vul in hoe vaak er evaluatiegesprekken met de serviceprovider plaatsvinden. Kies hierbij het antwoord dat het dichtst bij de werkelijkheid aansluit.

30. Heeft de serviceprovider over het tijdvak een **third party assurance** afgegeven?
    Vul in of de serviceprovider over het tijdvak een third party assurance heeft afgegeven.

31. Is de third party assurance over het tijdvak goedgekeurd door een externe auditor?
    Vul in of een externe auditor goedkeuring heeft gegeven op de third party assurance over het tijdvak. **Vul dit veld alleen in als u bij de vorige vraag 'Ja' heeft ingevuld. Laat het veld anders leeg.**

32. In welke mate dekt de scope van deze third party assurance verklaring de uitbestede dienstverlening?
    Vul in in welke mate de scope van de third party assurance verklaring de uitbestede dienstverlening dekt. **Vul dit veld alleen in als u bij vraag 5.4 'Ja' heeft ingevuld. Laat het veld anders leeg.**

33. Hebben zich er binnen het tijdvak incidenten voorgedaan bij de serviceprovider in relatie tot de **scheiding van omgevingen**?
    Vul in of er binnen het tijdvak ernstige incidenten hebben plaatsgevonden bij de serviceprovider als het gaat om de scheiding van omgevingen.

34. Hebben zich er binnen het tijdvak incidenten voorgedaan bij de serviceprovider in relatie tot **gegevenstoegang**?
    Vul in of er binnen het tijdvak ernstige incidenten hebben plaatsgevonden bij de serviceprovider als het gaat om gegevenstoegang.

35. Hebben zich er binnen het tijdvak **cyberincidenten** voorgedaan bij de serviceprovider?
    Vul in of er binnen het tijdvak ernstige incidenten hebben plaatsgevonden bij de serviceprovider als het gaat om cyberincidenten.

36. Hebben binnen het tijdvak ernstige incidenten bij de serviceprovider, genoemd onder AH-AJ geleid tot een verstoring van de dienstverlening van uw onderneming?
    Vul in of een van de incidenten zoals beschreven in de voorgaande drie vragen een verstoring of tijdelijke niet-beschikbaarheid van de dienstverlening van uw onderneming heeft veroorzaakt.

37. Verkeert de serviceprovider in financiële problemen?
    Vul in of de serviceprovider in financiële problemen verkeert voor zover dit bij uw onderneming bekend is.

38. Heeft uw onderneming gedurende het tijdvak een juridisch geschil gehad met de serviceprovider?
    Vul in of uw onderneming gedurende het tijdvak een juridisch geschil met de serviceprovider heeft gehad.

39. Voldeed de serviceprovider gedurende het tijdvak aan de overeengekomen **service levels**?
    Vul in of de serviceprovider gedurende het tijdvak voldeed aan de overeengekomen service levels in het contract. Kies voor de beschrijving die het best past bij uw ervaring met de serviceprovider.

40. In welke mate levert een overstap naar een andere serviceprovider risico's op voor de continuïteit van uw bedrijfsvoering?
    Vul in of een overstap naar een andere serviceproviders risico's oplevert voor de continuïteit van de dienstverlening van uw onderneming. Kies voor het antwoord dat het best past bij de situatie van uw onderneming.

41. Heeft uw onderneming de intentie om eerder dan de contractuele eind- of renewaldatum de samenwerking met de serviceprovider te beëindigen?
    Vul in of uw onderneming van plan is om eerder dan de contractueel vastgelegde eind- of renewaldatum de samenwerking met de serviceprovider te beëindigen.

42. Wat is de belangrijkste reden dat uw onderneming voortijdig het contract wil ontbinden?
    Vul in wat de belangrijkste reden is dat uw onderneming voor de contractuele eind- of renewaldatum de samenwerking met serviceprovider wil beëindigen. Kies voor het antwoord dat het best past bij de situatie van uw onderneming. **Vul dit veld alleen in als u bij de vorige vraag 'Ja' heeft ingevuld. Laat het veld anders leeg.**

Lijst van definities

Auditrecht	Een contractueel auditrecht houdt in dat uw onderneming zelf of door externen een audit mag (laten) uitvoeren op de beheersing van de processen van de dienstverlener.
BIV-classificatie	BIV is het acroniem voor Beschikbaarheid, Integriteit, Vertrouwelijkheid. Een BIV-classificatie is een indeling die binnen de informatiebeveiliging wordt gehanteerd, waarbij de beschikbaarheid (continuïteit), de integriteit (betrouwbaarheid) en de vertrouwelijkheid (exclusiviteit) van informatie en systemen wordt aangegeven.
BIV Beschikbaarheid	Beschikbaarheid: informatie moet beschikbaar en toegankelijk zijn. Deze classificatie gaat in op de mogelijke gevolgen als informatie, of een informatie set, niet beschikbaar is.
BIV Integriteit	Integriteit: het in overeenstemming zijn van informatie met de werkelijkheid (informatie is juist, volledig en actueel). Goed beheer van bevoegdheden en mogelijkheden tot muteren, toevoegen, of vernietigen van gegevens is cruciaal voor de integriteit van informatie. Deze classificatie gaat in op de mogelijke gevolgen wanneer informatie onjuist, onvolledig of niet actueel is.
BIV Vertrouwelijkheid	Vertrouwelijkheid: de bevoegdheden en mogelijkheden om kennis te nemen van informatie voor een gedefinieerde groep gerechtigden. Deze classificatie gaat in op de mogelijke gevolgen van de situatie waarin informatie in handen komt van derden die hiertoe niet zijn geautoriseerd.
Cyberincidenten	Cyberincidenten zijn incidenten waarbij de veiligheid van IT-systemen of data in het geding zijn gekomen. Hieronder vallen onder meer DDOS aanvallen, inbraken in IT-systemen en datalekken.
Exit clausule	Een exit clausule is een voorwaarde in een contract die het mogelijk maakt het contract eenzijdig open te breken en/of te ontbinden. De activering van de exit clausule kan bijvoorbeeld gekoppeld zijn aan de performance van de serviceprovider.
Gegevensopslag	De fysieke vastlegging van een gegevens op een drager, bij clouddiensten bijvoorbeeld de server of het datacentrum van de dienstverlener.
Gegevenstoegang	Gegevenstoegang ziet erop dat alleen geautoriseerde gebruikers toegang hebben tot de informatie waarvoor zij geautoriseerd zijn.
Gegevensverwerking	Elke handeling of elk geheel van handelingen met betrekking tot gegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen,

	gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens
Onderuitbesteding	Wanneer elementen van de uitbesteding door een ander dan en in opdracht van de hoofdserviceprovider worden uitgevoerd, is er sprake van onderuitbesteding.
Performance incentives	Performance incentives zijn contractuele afspraken over de prestaties van de serviceprovider. Performance incentives zijn onderverdeeld in twee soorten. De eerste soort is performance bonus, waarbij de serviceprovider een hogere vergoeding krijgt voor het nakomen van contractuele afspraken. De tweede soort is performance penalty, waarbij de serviceprovider een lagere vergoeding krijgt bij het niet nakomen van contractuele afspraken.
Risico Analyse	Een risicoanalyse is een methode waarbij risico`s worden gekwantificeerd door het bepalen van de kans dat een dreiging zich voordoet en de gevolgen daarvan: Risico = Kans x Gevolg.
Scheiding van omgevingen	De scheiding van omgevingen ziet erop dat IT-systemen en de bijbehorende databases afgescheiden zijn en blijven van andere IT-systemen en databases.
Service level	Een service level is een afspraak tussen een organisatie en een serviceprovider over de kwaliteit en prestatie-indicatoren die de serviceprovider moet leveren.
Serviceprovider	De toeleverancier of dienstverlener aan wie de financiële onderneming de uitvoering van een proces of één of meer bedrijfsactiviteiten uitbesteedt.
Third Party Assurance	Verklaring van een (vaak externe) auditor dat een bepaalde dienstverlening voldoet aan algemeen geldende beheersingsprincipes. In de verklaring is de scope en het tijdvak opgenomen waarover de verklaring is afgegeven.
Third Party Assurance type 2	Een third party assurance type 2 verklaring geeft assurance over een bepaalde tijdsperiode. Dit in tegenstelling tot een type 1 verklaring. Een type 1 verklaring is een momentopname.

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