AFM

Werkwijze Autoriteit Financiële Markten met betrekking tot het inzien en kopiëren van digitale gegevens

1) Inleiding
Ingevolge artikel 29, derde lid, van de Wet toezicht effectenverkeer 1995 ('Wte 1995'), artikel 19, derde lid, van de Wet toezicht beleggingsinstellingen ('Wtb') en artikel 69 van de Wet financiële dienstverlening ('Wfd') juncto artikel 5:17, eerste lid, van de Algemene wet bestuursrecht ('Awb') hebben de personen die door de Autoriteit Financiële Markten ('AFM') zijn belast met het inwinnen van inlichtingen of met de uitoefening van andere taken en bevoegdheden die de AFM heeft op grond van het bepaalde bij en krachtens de Wte 1995, Wtb en Wfd, de bevoegdheid inzage te vorderen van zakelijke gegevens en bescheiden. Ingevolge artikel 5:17, tweede lid, Awb hebben zij tevens de bevoegdheid kopieën te maken van de betreffende gegevens en bescheiden. De AFM acht het wenselijk duidelijkheid te verschaffen omtrent de wijze waarop invulling wordt gegeven aan de aan artikel 5:17, eerste en tweede lid, Awb ontleende bevoegdheden om digitale gegevens en bescheiden in te zien en te kopiëren. Daartoe is deze werkwijze opgesteld.

2) Definities
In deze werkwijze wordt verstaan onder:
a) Digitale kopie: Een kopie van een digitaal opgeslagen bestand of een selectie uit een groter bestand.
b) Forensische image: Een integrale kopie van digitaal opslagmedium, waardoor tevens inzage kan worden verkregen in de digitale bestanden waartoe de gebruiker geen toegang (meer) heeft (zoals verwijderde bestanden), de historie van bestanden (bijvoorbeeld eerdere versies) en de digitale omgeving van bestanden (bijvoorbeeld de status daarvan).
c) Gebruikersbestand: Bestand dat mogelijk door een gebruiker is aangemaakt. Bestand kan ook bestaan uit een collectie van voor de gebruiker losse objecten, zoals een bestand met meerdere berichten. Het feitelijke bestand hoeft niet voor de gebruiker benaderbaar te zijn.
d) HASH-waarde of controle totaal: Een unieke waarde, welke algoritmisch wordt berekend over digitale kopieën en/of forensische images. Aan de hand van deze unieke waarde kan de authenticiteit (HASH-waarde) of plausibiliteit (controle totaal) van digitale kopieën en/of forensische images achteraf worden gecontroleerd.
e) Indexeren: Het maken van een inhoudsopgave, welke het mogelijk maakt gericht te zoeken in een gegevensverzameling.
f) Opslagmedia: Gegevensdragers zoals harde schijven, diskettes, cd-rom's
g) Database: Gegevensverzameling waarbij de gegevens zijn verdeeld over tabellen die op een logische manier met elkaar samenhangen en in relatie staan tot elkaar.
h) Privé-gegevens: Gegevens van persoonlijke aard, welke niet worden gebruikt ten dienste van het maatschappelijk verkeer of zakelijke doeleinden. Ten aanzien van deze gegevens is artikel 5:17 Awb niet van toepassing.
i) Geprivilegieerde gegevens: Gegevens met betrekking tot de toepassing van regels op de naleving waarvan de AFM toezicht houdt, gewisseld tussen een onderneming en een advocaat die is toegelaten tot de balie, die zich bij onderneming bevinden, doch waarop, indien zij zich zouden bevinden bij de advocaat, artikel 5:20, tweede lid, Awb van toepassing zou zijn. Ten aanzien van deze gegevens is artikel 5:17 Awb niet van toepassing.
j) Werkkopie: Een ten kantore van de AFM gemaakte kopie van de bij of door de onderneming gemaakte digitale kopieën en forensische images, welke als basis dient voor de onder 4, sub b, en verder genoemde werkzaamheden.

3) Procedure inzake het verkrijgen van digitale gegevens van een onderneming
a) Het maken van forensische images en digitale kopieën door de AFM vindt uitsluitend plaats door op dit werkterrein deskundige toezichthouders van de AFM, dan wel door specialisten die hiervoor zijn ingehuurd. In afwijking van het voorgaande kan de AFM ook gebruik maken van forensische images of digitale kopieën die door de onderneming zelf zijn gemaakt, en die op verzoek van de AFM aan haar worden verstrekt.
b) Kennis omtrent wachtwoorden, protocollen en andere aspecten van het ontsluiten van data dient in de vorm van een systeem- en of databasebeheerder beschikbaar te zijn.
c) Van opslagmedia van de voor het onderzoek van belang zijnde personen, kan een forensische image worden gemaakt. Aan die forensische image wordt een code gekoppeld, de zogenaamde HASH-waarde. Dit garandeert de authenticiteit van de gegevens op de forensische image; de code verandert zodra er iets in het opslagmedium wordt gewijzigd. Het maken van een kopie van het gehele opslagmedium (inclusief omgeving) is onder meer nodig om (i) de onderdelen te kunnen relateren, en (ii) de eventuele op het opslagmedium verwijderde documenten terug te halen. Het maken van een forensische image kan enige tijd (in zijn algemeenheid betreft het enkele uren) in beslag nemen. Gedurende deze tijd kunnen de gebruikers geen gebruik maken van de opslagmedia.
d) Voorts kan een digitale kopie worden gemaakt van de bestanden of een selectie uit een database, zonder de omgeving te kopiëren (zoals bij een forensische image het geval is). Van de betreffende bestanden wordt geen forensische image gemaakt, aangezien het doorgaans bestanden op een server betreft. Het maken van een forensische image van de server is, gelet op de tijdsbeslag en gelet op het feit dat veel personen gebruik maken van de server, in de regel niet opportuun.
e) Van opgevraagde bestanden dient een beschrijving te worden verstrekt. Deze beschrijving dient voor zover van toepassing, te bevatten: veldnamen, rekenregels, plausibiliteitscontroles, controletotalen en andere aspecten van deze bestanden.
f) Zowel de digitale kopieën als de

forensische images zijn niets anders dan kopieën ten behoeve van het onderzoek van de AFM. De onderneming blijft in het bezit van de originele bestanden en opslagmedia.
g) Indien de onderneming verzoekt om geprivilegieerde of privé-gegevens te verwijderen uit digitale kopieën, dan zal de AFM daartoe overgaan. Daarbij gelden de volgende voorwaarden:

(1) Indien het een bezoek van de AFM ter plaatse bij de onderneming betreft, dient het verzoek niet onnodig vertragend zijn voor de te verrichten handelingen ter plaatse. Als dit wel zo is zal het verzoek ten kantore van de AFM worden uitgevoerd;

(2) De instelling dient concreet aan te geven om welke bestanden het gaat of een lijst verstrekken met concrete zoektermen, waarmee de AFM geprivilegieerde of privé bestanden kan identificeren;

(3)De toezichthouder dient zich ervan te vergewissen dat de selectie daadwerkelijk geprivilegieerde of privé-informatie bevat.

Vervolgens wordt een nieuwe digitale kopie gemaakt van de gefilterde oorspronkelijke kopie. Daarmee wordt gegarandeerd dat de verwijderde data door digitale technieken niet alsnog deel uitmaken van de onderzoeksdata.
h) Ten aanzien van geprivilegieerde of privé-gegevens in forensische images is het niet mogelijk ter plaatse de betreffende bestanden te verwijderen, aangezien met het verwijderen van gegevens de digitale omgeving zou veranderen. De onderneming zal daarom in een later stadium worden uitgenodigd ten kantore van de AFM de handelingen bij te wonen waarmee de AFM de betreffende bestanden uit de werkkopieën verwijdert. Indien de onderneming gebruik wil maken van de mogelijkheid de onder g. genoemde handelingen bij te wonen, dan dient de onderneming uiterlijk binnen één week na het onderzoek ter plaatse dit schriftelijk kenbaar te maken aan de AFM.
i) Indien, tijdens een bezoek van de AFM ter plaatse forensische images worden gemaakt, verstrekken de toezichthouders van de AFM aan de onderneming de namen van de leveranciers van de software die de AFM gebruikt om de forensische images te maken en in te zien. Op deze wijze kan de onderneming op een zelfde wijze toegang krijgen tot de (al dan niet verwijderde) gekopieerde bestanden.
j) Indien de gegevens zijn verkregen bij een bezoek van de AFM ter plaatse bij de onderneming, wordt ten kantore van de AFM een verslag van handelingen opgemaakt.

4) Procedure ten kantore van de AFM
a) Na het verkrijgen van de digitale gegevens worden ten kantore van de AFM de forensische images met de bijbehorende HASH-waarde alsmede de digitale kopieën in behandeling genomen door op dit werkterrein deskundige toezichthouders van de AFM. De toezichthouder maakt vervolgens van alle forensische images en digitale kopieën een werkkopie, waarna de originele forensische images en digitale kopieën in een kluis worden opgeborgen. Ten aanzien van de originele forensische images en digitale kopieën worden uitsluitend beheerswerkzaamheden verricht om het instandhouden van de informatie te garanderen. De opgeslagen informatie blijft tijdens die beheerswerkzaamheden onaangeroerd.

Voorbereidende werkzaamheden
b) De eerstvolgende stappen bestaan uit het door de op dit werkterrein deskundige toezichthouders van de AFM voorbereiden van de data uit de werkkopie voor de AFM-onderzoekers, teneinde hen in een later stadium in de gelegenheid te stellen gericht te zoeken in het digitale materiaal. Tijdens deze voorbereidende werkzaamheden wordt nog geen inhoudelijk onderzoek. De voorbereidende werkzaamheden kunnen geruime tijd in beslag nemen. De duur kan – afhankelijk van beslissingen omtrent organisatie en prioritering – enkele weken tot enkele maanden beslaan.
c) Aan de hand van specialistische programmatuur worden ten aanzien van gebruikersbestanden voorbereidende werkzaamheden verricht, welke de AFM-onderzoekers in een later stadium in de gelegenheid moeten stellen kennis te kunnen nemen van de inhoud van de betreffende bestanden. Een aantal documenten zal daarbij worden verwijderd. Dit betreft documenten die niet (meer) leesbaar zijn te maken en documenten die gezien hun aard bij voorbaat niet relevant kunnen zijn voor het uiteindelijke AFM-onderzoek.
d) De onder 4, sub c, geselecteerde gebruikersbestanden worden vervolgens geïndexeerd. Door middel van het indexeren wordt de inhoud van bestanden toegankelijk gemaakt voor het gericht zoeken door de AFM-onderzoekers. Bestanden die op deze wijze niet toegankelijk kunnen worden gemaakt[1], worden separaat en buiten de index ter beschikking gesteld.
e) In geval van vragen zal contact opgenomen worden met de instelling of (externe) beheerders van de relevante applicaties.

Geprivilegieerde of privé-gegevens
f) Indien tijdens het ophalen van gegevens ter plaatse verwijdering van geprivilegieerde of privé-gegevens niet heeft plaatsgevonden en indien de onderneming binnen één week na het onderzoek ter plaatse schriftelijk aan de AFM kenbaar heeft gemaakt dat zij prijs stelt op het aanleveren van een overzicht met documenten die dergelijke gegevens bevatten, verzendt de AFM aan de onderneming een kennisgeving om haar ten kantore van de AFM die gelegenheid te bieden. De onderneming kan vervolgens aan de hand van een met de kennisgeving door de AFM meegezonden overzicht van toegankelijke bestanden aangeven om welke bestanden het gaat. Zij kan ook een lijst met concrete zoektermen verstrekken, waarmee de AFM geprivilegieerde of privé-gegevens moet kunnen identificeren. Indien gegevens worden verwijderd, zullen de onderzoeksdata opnieuw worden geïndexeerd. Daarmee wordt gegarandeerd dat de verwijderde data door digitale technieken niet alsnog deel uitmaken van de onderzoeksdata[2].

Gerichte zoekacties
g) De AFM zendt aan de onderneming een kennisgeving dat haar de gelegenheid wordt geboden aanwezig te zijn bij gerichte zoekacties in het digitale materiaal, dan wel in beginsel binnen één week na de gerichte zoekacties een afschrift van de lijst met gehanteerde zoektermen te ontvangen.
h) De AFM-onderzoekers gaan over tot daadwerkelijke inzage in de toegankelijk gemaakte onderzoeksdata. De gerichte zoekacties in het digitale

materiaal vinden plaats ten kantore van de AFM in een daarvoor ingerichte ruimte. De gerichte zoekacties vinden plaats aan de hand van een lijst met zoektermen, welke in overeenstemming is met de doelstellingen van het onderzoek. De onderneming krijgt tijdens de gerichte zoekacties inzage in de zoektermen die worden ingevoerd. Zij krijgt geen inzage in de zoekresultaten.
i) Het is mogelijk dat meerdere malen de digitale onderzoeksdata dienen te worden geraadpleegd, aangezien inzage in bepaalde documenten kan leiden tot andere aanwijzingen binnen het onderzoek, die aanleiding geven tot aanvullend onderzoek. De onderneming zal bij herhaalde raadpleging opnieuw in de gelegenheid worden gesteld deze gerichte zoekacties bij te wonen, dan wel een lijst met zoektermen te ontvangen, op de wijze zoals beschreven onder 4, sub h en sub i.

Van de onderzoekshandelingen wordt achteraf een verslag van verrichte handelingen opgemaakt.

5) Bewaring en vernietiging van digitale gegevens
De digitale gegevens waarover de AFM de beschikking krijgt worden bewaard en uiteindelijk vernietigd overeenkomstig het bepaalde bij en krachtens de Archiefwet 1995.

6) Inwerkingtreding
Deze werkwijze treedt in werking met ingang van de dag na publicatie ervan in de Nederlandse Staatscourant.

Amsterdam, 19 juli 2006.
Autoriteit Financiële Markten,
A.W.H. Docters van Leeuwen.
A.W. Kist.

[1] Te denken valt aan boekhoudkundige systemen en relationele databases.
[2] Indien het onderzoek van de AFM resulteert in (het voornemen tot) een besluit tot het opleggen van een handhavingsmaatregel, dan zullen de zoekresultaten welke relevant zijn voor het onderzoek deel gaan uitmaken van de op de zaak betrekking hebbende stukken, welke te zijner tijd ter inzage zullen worden gelegd in het kader van de zienswijze- en/of bezwaarschriftprocedure.