



## Werkwijze AFM inzien en kopiëren van digitale gegevens

### Begripsomschrijvingen

*Digitale gegevens:* gegevens waarover de onderneming in elektronische vorm beschikt of kan beschikken.

*Functionaris verschoningsrecht:* een door het bestuur van de Autoriteit Financiële Markten (AFM) aangewezen persoon die niet als toezichthouder bij onderzoeken betrokken is of zal zijn en het geprivilegieerde karakter van de door de onderneming als zodanig geclaimde gegevens toetst.

*Geprivilegieerde gegevens:* gegevens die zijn gewisseld tussen een onderneming en een advocaat die is toegelaten tot de balie. De gegevens worden als geprivilegieerd aangemerkt wanneer de advocaat zich ten aanzien van die gegevens zou kunnen beroepen op het verschoningsrecht zoals vastgelegd in artikel 5:20, tweede lid, Awb, indien de gegevens zich bij hem/haar zouden bevinden.<sup>1</sup>

*Geschoonde gegevens:* digitale gegevens zoals gekopieerd door de toezichthouder (in voorkomend geval de IT-specialist), met uitzondering van eventuele verwijderde privé- en/of geprivilegieerde gegevens.

*IT-specialist:* toezichthouder belast met de technische bewerking van digitale gegevens die zich niet bezighoudt met de inhoudelijke behandeling van het onderzoek.

*Privé gegevens:* gegevens en bescheiden van persoonlijke aard die niet worden gebruikt ten dienste van het maatschappelijk verkeer.

*Toezichthouder:* een door het bestuur van de AFM aangewezen functionaris belast met het houden van toezicht.

*Werkwijze:* de Werkwijze AFM inzien en kopiëren van digitale gegevens.

### 1 – Inleiding

Met toezicht op de naleving van de bij en krachtens (onder meer) de Wet op het financieel toezicht (Wft) gestelde regels zijn belast de bij besluit van de AFM aangewezen personen.<sup>2</sup> Deze door de AFM aangewezen personen beschikken over de bevoegdheid die de Algemene wet bestuursrecht (Awb) toekent om inzage te vorderen van zakelijke gegevens en bescheiden en daarvan kopieën te maken.<sup>3</sup> Ook zijn zij bevoegd om inlichtingen te vorderen.<sup>4</sup> De onderneming waarbij een onderzoek wordt verricht, is verplicht medewerking te verlenen aan het uitoefenen van die bevoegdheid voor zover dat wordt gevorderd.<sup>5</sup>

Deze Werkwijze geeft op hoofdlijnen weer hoe de toezichthouders van de AFM te werk zullen gaan bij het uitoefenen van genoemde bevoegdheden voor zover de AFM daarbij digitale gegevens vordert. De Werkwijze is van overeenkomstige toepassing op het vorderen van digitale gegevens op grond van artikel 5:16 Awb, in andere situaties dan tijdens een onderzoek ter plaatse. De Werkwijze beschrijft de gevolgde procedure vanaf het moment dat de digitale gegevens door de toezichthouders zijn geselecteerd die naar hun aard en/of inhoud redelijkerwijs binnen het doel en voorwerp van het betreffende onderzoek kunnen vallen.

### 2 – Het identificeren van privé- en geprivilegieerde gegevens

1. De toezichthouder stelt de onderneming, in beginsel tijdens het onderzoek ter plaatse, in de gelegenheid aan te geven of de door de toezichthouder geselecteerde digitale gegevens privé- en/of geprivilegieerde gegevens bevatten.
2. Indien de onderneming aangeeft dat de door de toezichthouder geselecteerde digitale gegevens geen privé- en/of geprivilegieerde gegevens bevatten, of de onderneming aangeeft afstand te willen doen van de bescherming van privé- en geprivilegieerde gegevens, en het identificeren als

<sup>1</sup> Onder het verschoningsrecht valt bijvoorbeeld niet correspondentie met juridische adviseurs (waaronder bedrijfsjuristen) die geen advocaat zijn en correspondentie met advocaten die niet zijn ingeschreven bij de balie van een lidstaat van de Europese Unie. Als een bedrijfsjurist ook advocaat is, moet uit de geprivilegieerde documenten duidelijk blijken dat de bedrijfsjurist als advocaat handelt. De bedrijfsjurist is hier zelf verantwoordelijk voor. Wel vallen onder het verschoningsrecht eventuele interne documenten voor zover daarin de correspondentie met voornoemde advocaten is weergegeven of samengevat en interne documenten die zijn opgesteld met het uitsluitend doel om advies van die advocaat in te winnen.

<sup>2</sup> Artikel 5:11 Awb jo artikel 1:72 Wft. Verwezen wordt naar de regeling van mandaat, volmacht en machtiging van de AFM zoals laatstelijk gewijzigd. In die regeling wordt gedetailleerd omschreven welke bevoegdheden het bestuur van de AFM heeft geman-dateerd en aan welke personen.

<sup>3</sup> Artikel 5:17 Awb.

<sup>4</sup> Artikel 5:16 Awb.

<sup>5</sup> Artikel 5:20, eerste lid, Awb.



bedoeld onder 1 van deze paragraaf aldus achterwege kan worden gelaten, bevestigt de toezichthouder dit schriftelijk aan de onderneming binnen vijf werkdagen na het onderzoek ter plaatse. De toezichthouder kopieert de geselecteerde digitale gegevens naar een opslagmedium van de AFM.

3. Indien de onderneming gemotiveerd aangeeft dat de geselecteerde digitale gegevens wel privé- en/of geprivilegieerde gegevens bevatten, vergewist de IT-specialist zich – behoudens het bepaalde onder 7 ten aanzien van geprivilegieerde gegevens – van de juistheid van deze claim door deze ter plaatse vluchtig in te zien.
4. Indien de IT-specialist op basis van het vluchtig inzien van de als privé of geprivilegieerd geclaimde digitale gegevens overtuigd is van het privé- of geprivilegieerd karakter verwijderd hij de betreffende gegevens uit de geselecteerde gegevens.
5. Indien de IT-specialist op basis van het vluchtig inzien van de als privé geclaimde digitale gegevens niet overtuigd is van het privé karakter, kopieert de IT-specialist de geselecteerde digitale gegevens inclusief de als privé geclaimde digitale gegevens naar een opslagmedium van de AFM en voegt deze toe aan het onderzoeksdossier.
6. Indien de IT-specialist op basis van het vluchtig inzien van de als geprivilegieerd geclaimde digitale gegevens niet overtuigd is van het geprivilegieerde karakter, terwijl de onderneming zijn claim wel handhaaft, verzoekt de IT-specialist de onderneming zijn claim schriftelijk nader te motiveren binnen tien werkdagen na het onderzoek ter plaatse. De onderneming dient de motivering uitsluitend te richten aan de functionaris verschoningsrecht en daarbij duidelijk aan te geven dat en waarom het geprivilegieerde informatie betreft.<sup>6</sup>

Dit motiveren bestaat ten minste uit het aangeven:

- wie de digitale gegevens heeft opgesteld,
- aan wie deze zijn gericht,
- wat de functies en verantwoordelijkheden van deze personen zijn,
- wat het doel van de digitale gegevens is en in welke context deze zijn opgesteld.

De IT-specialist kopieert de als geprivilegieerd geclaimde digitale gegevens afzonderlijk van de overige geselecteerde digitale gegevens naar een opslagmedium van de AFM. De als geprivilegieerd geclaimde digitale gegevens worden overhandigd aan de functionaris verschoningsrecht en worden door de toezichthouder niet verder ingezien tot het moment dat door de functionaris verschoningsrecht definitief is beoordeeld of de claim al dan niet terecht is en de gegevens waarvan de functionaris verschoningsrecht heeft geoordeeld dat de claim niet terecht is aan het onderzoeksdossier zijn toegevoegd conform de procedure beschreven in paragraaf 3.

7. Indien de onderneming stelt dat zelfs het vluchtig inzien van de als geprivilegieerd geclaimde gegevens door de toezichthouder het geprivilegieerde karakter al kan schaden, verzoekt de toezichthouder de onderneming zijn claim schriftelijk nader te motiveren binnen tien werkdagen na het onderzoek ter plaatse. Dit motiveren bestaat ten minste uit het aangeven van de elementen genoemd onder 6 van deze paragraaf, aangevuld met het aangeven waarom het vluchtig inzien al het geprivilegieerde karakter van de betreffende digitale gegevens kan schaden. De onderneming dient de motivering uitsluitend te richten aan de functionaris verschoningsrecht en daarbij duidelijk aan te geven dat en waarom het geprivilegieerde informatie betreft.  
De IT-specialist kopieert de als geprivilegieerd geclaimde digitale gegevens afzonderlijk van de overige geselecteerde digitale gegevens naar een opslagmedium van de AFM zonder deze in te zien. De als geprivilegieerd geclaimde digitale gegevens worden overhandigd aan de functionaris verschoningsrecht en worden door de toezichthouder niet ingezien tot het moment dat door de functionaris verschoningsrecht definitief is beoordeeld of de claim al dan niet terecht is en de gegevens waarvan de functionaris verschoningsrecht heeft geoordeeld dat de claim niet terecht is aan het onderzoeksdossier zijn toegevoegd conform de procedure beschreven in paragraaf 3.
8. Indien het identificeren van privé- en/of geprivilegieerde digitale gegevens als bedoeld onder 1 van deze paragraaf in de ogen van de toezichthouder tot onnodige vertraging leidt voor de te verrichten handelingen ter plaatse of op andere zwaarwegende praktische bezwaren stuit, kopieert de IT-specialist de geselecteerde digitale gegevens naar een opslagmedium van de AFM zonder deze in te zien. De toezichthouder stelt de onderneming in de gelegenheid binnen tien werkdagen na het onderzoek ter plaatse, schriftelijk gemotiveerd aan te geven welke van de geselecteerde digitale gegevens privé en/of geprivilegieerd zijn.  
De geselecteerde digitale gegevens zullen niet worden ingezien door de toezichthouder tot het moment dat voornoemde motivering binnen de daarvoor gestelde termijn van de onderneming door de AFM is ontvangen. Na ontvangst van de motivering wordt in lijn met de hierboven en hierna beschreven procedure gehandeld. De onderneming wordt in dat geval door de AFM in de gelegenheid gesteld ten kantore van de AFM aanwezig te zijn bij de onder 3 van deze paragraaf genoemde handelingen. De onderneming dient binnen tien werkdagen na het onderzoek ter plaatse aan de AFM te laten weten of zij bij de genoemde handelingen aanwezig wenst te zijn.

<sup>6</sup> Voor zover digitale gegevens worden gevorderd op grond van artikel 5:16 Awb, in andere situaties dan tijdens een onderzoek ter plaatse, vermeldt de toezichthouder bij zijn vordering dat digitale gegevens waarvan geclaimd wordt dat deze geprivilegieerd zijn, rechtstreeks aan de functionaris verschoningsrecht dienen te worden gestuurd.



### **3 – Het beoordelen van de claim door de functionaris verschoningsrecht**

1. De functionaris verschoningsrecht toetst het geprivilegieerde karakter van de door de onderneming overeenkomstig paragraaf 2 onder 6 of 7 als zodanig geclaimde digitale gegevens. De door de functionaris verschoningsrecht in het kader van de claims gevoerde correspondentie is niet toegankelijk voor de toezichthouder.
2. Voor zover de functionaris verschoningsrecht van oordeel is dat de claim terecht is, stelt hij de onderneming daarvan schriftelijk in kennis en laat hij de desbetreffende digitale gegevens vernietigen door een IT-specialist.
3. Voor zover de functionaris verschoningsrecht van oordeel is dat de claim niet terecht is, stelt hij de onderneming daarvan schriftelijk en gemotiveerd in kennis. Indien de onderneming de claim desalniettemin wenst te handhaven, verzoekt hij de onderneming daarbij om binnen tien werkdagen na verzending van die schriftelijke kennisgeving zijn standpunt schriftelijk nader toe te lichten. De onderneming dient de betreffende correspondentie uitsluitend te richten aan de functionaris verschoningsrecht en daarbij duidelijk aan te geven dat het geprivilegieerde informatie betreft.
4. Indien de onderneming in de claim volhardt en een nadere toelichting toestuurt als bedoeld in het vorige lid, beoordeelt de functionaris verschoningsrecht het geprivilegieerde karakter van de door de onderneming als zodanig geclaimde digitale gegevens nogmaals met inachtneming van die toelichting.
5. Is de functionaris verschoningsrecht na deze nadere toelichting alsnog van oordeel dat de claim terecht is, dan laat hij de desbetreffende digitale gegevens vernietigen door een IT-specialist. De functionaris verschoningsrecht stelt de onderneming schriftelijk in kennis van zijn beoordeling.
6. Blijft de functionaris verschoningsrecht na deze nadere toelichting van oordeel dat de claim onterecht is, dan stelt hij de onderneming daarvan schriftelijk in kennis. In deze kennisgeving geeft de functionaris verschoningsrecht aan dat de desbetreffende digitale gegevens niet eerder dan tien werkdagen na verzending van de kennisgeving zullen worden toegevoegd aan het onderzoeksdossier. De wachtermijn van in elk geval tien dagen dient ertoe de onderneming de mogelijkheid te bieden een kort geding aanhangig te maken bij de civiele rechter.

### **4 – Gerichte zoekacties**

1. De gerichte zoekacties worden uitgevoerd in de geschoonde gegevens ten kantore van de AFM door middel van zoektermen die verband houden met het doel en voorwerp van onderzoek.
2. De lijst met tijdens het onderzoek gehanteerde zoektermen wordt opgenomen in het dossier. Op verzoek van de onderneming wordt de onderneming een afschrift van de lijst met gehanteerde zoektermen gestuurd binnen een week nadat het gericht zoeken in het desbetreffende onderzoek is afgerond. De onderneming krijgt geen inzage in de zoekresultaten.
3. In het geval dat de toezichthouder tijdens het onderzoek privé en/of geprivilegieerde digitale gegevens aantreft die niet als zodanig zijn geclaimd en derhalve niet zijn beoordeeld overeenkomstig paragraaf 2 en 3 van de Werkwijze, zal hij deze tijdens het onderzoek terzijde laten. Deze digitale gegevens worden vernietigd conform het bepaalde onder paragraaf 5 van de Werkwijze.

### **5 – Vernietiging van digitale gegevens**

Na afronding van het onderzoek en nadat eventuele bezwaar- of beroepstermijnen met betrekking tot besluiten die naar aanleiding van het onderzoek zijn genomen zijn verstreken of, indien bezwaar is gemaakt of beroep is ingesteld, op dat bezwaar of beroep onherroepelijk is beslist, laat de functionaris verschoningsrecht de uitgewisselde correspondentie tussen hem en de onderneming over de als geprivilegieerd geclaimde gegevens evenals de gegevens waarvan is vast komen te staan dat deze geprivilegieerd zijn (voor zover die gegevens niet al vernietigd zijn, zie paragraaf 3 onder 2 en 5) vernietigen door een IT-specialist. De toezichthouder vernietigt vervolgens alle digitale gegevens met uitzondering van die gegevens die in het rapportdossier zijn opgenomen.

### **6 – Intrekking eerdere werkwijze**

De 'Werkwijze Autoriteit Financiële Markten met betrekking tot het inzien en kopiëren van digitale gegevens', gepubliceerd in de Staatscourant van 21 juli 2006, wordt ingetrokken.



---

## 7 – Inwerkingtreding

Deze Werkwijze treedt in werking met ingang van de eerste dag na dagtekening van de Staatscourant waarin deze wordt geplaatst.

*Autoriteit Financiële Markten,  
J.F. Hoogervorst MA,  
Bestuursvoorzitter.*

*T.F. Kockelkoren MBA,  
Bestuurslid.*