



Werkwijze AFM inzien en kopiëren van digitale gegevens

Artikel 1 – Definitiebepalingen

Awb: de Algemene wet bestuursrecht.

Digitale gegevens: elektronische gegevens waarover het Onderzoekssubject beschikt of kan beschikken.

Functionaris Verschoningsrecht: een door het bestuur van de Autoriteit Financiële Markten (AFM) aangewezen persoon die niet als IT-Specialist of als Onderzoeker bij toezichtonderzoeken betrokken is of zal zijn, maar onafhankelijk, met technische ondersteuning van de IT-Specialist, het geprivilegieerde karakter van de door het Onderzoekssubject als zodanig geclaimde gegevens toetst.

Geprivilegieerde gegevens: Digitale gegevens die zijn gewisseld tussen een Onderzoekssubject en diens advocaat¹ in die hoedanigheid. 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 en hij over die gegevens kan beschikken.

Geschoonde gegevens: Digitale gegevens zoals veiliggesteld en gekopieerd door de IT-Specialist waarvan Geprivilegieerde- en/of Privégegevens zijn uitgesloten.

IT-Specialist: een toezichthouder in de zin van artikel 5:11 Awb die niet betrokken is bij de inhoudelijke uitvoering van het toezichtonderzoek, maar belast is met het proces van identificeren, veiligstellen, kopiëren en verwerken van Digitale gegevens, waaronder het technisch voorbereiden dan wel uitvoeren van de Schoning.

Onderzoeker: een toezichthouder in de zin van artikel 5:11 Awb die het toezichtonderzoek uitvoert.

Onderzoekssubject: de natuurlijke persoon of rechtspersoon die betrokken is bij activiteiten waarop door de AFM wordt toegezien ingevolge de wettelijke regeling op grond waarvan zij als toezichthouder belast is.

Privégegevens: Digitale gegevens en bescheiden van niet-zakelijke aard die betrekking hebben op de privésituatie. Artikel 5:17 Awb is hierop niet van toepassing.

Schonen / Schoning: het uitsluiten van Geprivilegieerde- en/of Privégegevens uit de verzameling van veiliggestelde en gekopieerde digitale gegevens.

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

Artikel 2 – Identificeren, veiligstellen en kopiëren van Digitale gegevens

1. De Onderzoeker stelt, aan de hand van het doel van het toezichtonderzoek, vast welke Digitale gegevens worden gevorderd. De IT-Specialist draagt er zorg voor dat deze Digitale gegevens worden geïdentificeerd, veiliggesteld en gekopieerd.
2. De gekopieerde Digitale gegevens worden door de IT-Specialist op versleutelde wijze getransporteerd naar de AFM en worden ten kantore van de AFM opgeslagen op een van het toezicht afgescheiden IT-omgeving. De Onderzoeker heeft geen toegang tot de digitale gegevens.
3. De IT-Specialist verstrekt binnen vijf werkdagen na het kopiëren van de digitale gegevens een overzicht van de gekopieerde Digitale gegevens en wijst het Onderzoekssubject op de mogelijkheid tot Schonen van gekopieerde Digitale gegevens zoals genoemd in het vierde en zesde lid.
4. Indien het Onderzoekssubject claimt dat de Digitale gegevens Geprivilegieerde gegevens bevatten, kan zij² de AFM schriftelijk verzoeken om deze gegevens te Schonen. Dit verzoek dient te worden gericht aan de IT-Specialist of, indien toepassing wordt gegeven aan artikel 3, zesde lid, van de Werkwijze, aan de Functionaris Verschoningsrecht. Het verzoek dient uiterlijk 10 werkdagen na verzending van de in het derde lid genoemde kennisgeving te zijn ontvangen door voornoemde functionarissen.
5. Het in het vierde lid genoemde verzoek dient ten minste de volgende informatie te bevatten:

¹ Waar in de definitiebepaling advocaat staat kan ook arts, notaris of geestelijke gelezen worden.

² Dit verzoek kan door zowel het Onderzoekssubject als door de verschoningsgerechtigde zelf worden gedaan. In verband hiermee kan, daar waar het in de Werkwijze gaat over het Onderzoekssubject en (de beoordeling van) de claim tot Schonen, ook de verschoningsgerechtigde worden gelezen.

- a. een overzicht van domeinnamen en/of e-mailadressen op basis waarvan Geprivilegieerde gegevens kunnen worden geïdentificeerd³, en
 - b. een deugdelijke onderbouwing waaruit blijkt dat er sprake is van Geprivilegieerde gegevens.
6. Het in het vierde lid genoemde verzoek kan ook gedaan worden ten aanzien van een claim dat de Digitale gegevens Privégegevens bevatten.
7. Het in het zesde lid genoemde verzoek dient ten minste de volgende informatie te bevatten:
- a. een overzicht van domeinnamen en/of e-mailadressen op basis waarvan Privégegevens kunnen worden geïdentificeerd⁴, en
 - b. een deugdelijke onderbouwing waaruit blijkt dat er sprake is van Privégegevens.
8. Indien het Onderzoekssubject nalaat binnen 10 werkdagen na verzending van de in het derde lid genoemde kennisgeving, een verzoek voor Schoning te doen, zoals bedoeld in het vierde en/of zesde lid, of binnen voornoemde termijn aangeeft geen verzoek te willen doen, bevestigt de IT-Specialist dit schriftelijk aan het Onderzoekssubject. De IT-Specialist voert, indien nodig, een pro-forma Schoning van Geprivilegieerde gegevens uit, waarna het toezichtonderzoek in de Geschoonde gegevens gestart kan worden overeenkomstig het gestelde in artikel 5.

Artikel 3 – Beoordelen van de claim door de IT-Specialist

1. De IT-Specialist beoordeelt geclaimde Geprivilegieerde- en/of Privégegevens uit de gekopieerde Digitale gegevens aan de hand van de onderbouwing zoals bedoeld in artikel 2, vijfde lid, onder b, of artikel 2, zevende lid, onder b, van de Werkwijze. Hierbij zal de IT-Specialist, door kennis te nemen van metadata en, waar nodig, door middel van vluchtig inzien, beoordelen of de claim aannemelijk is.
2. De Schoning vindt in beginsel plaats ten kantore van de AFM. Indien het Onderzoekssubject ondubbelzinnig en met precisie Geprivilegieerde- en/of Privégegevens kan duiden, dan zal de Schoning ten kantore van het Onderzoekssubject worden uitgevoerd, tenzij dit naar het oordeel van de IT-Specialist op technische of andere zwaarwegende praktische bezwaren stuit.
3. Indien de Schoning ten kantore van de AFM wordt uitgevoerd, zal de IT-Specialist technische voorbereidingen treffen waarna het Onderzoekssubject in de gelegenheid wordt gesteld om, ten kantore van de AFM, een mondelinge toelichting te krijgen over de wijze waarop de Schoning is voorbereid en zal worden afgewikkeld.
4. Indien het verzoek, zoals bedoeld in artikel 2, vierde en/of zesde lid, van de Werkwijze, onvoldoende aanknopingspunten geeft om de Schoning uit te voeren, wordt het Onderzoekssubject eenmalig in de gelegenheid gesteld om binnen een termijn van 5 werkdagen een aanvullende toelichting te geven.
5. Indien de IT-Specialist van oordeel is dat de claim (of een deel daarvan) zoals bedoeld in artikel 2, vierde en/of zesde lid, van de Werkwijze, al dan niet aannemelijk is, stelt de IT-Specialist het Onderzoekssubject daarvan schriftelijk in kennis en schoont de IT-Specialist de digitale gegevens waarvan de claim aannemelijk is.
6. Indien het Onderzoekssubject gefundeerd aangeeft dat hij niet wenst dat de IT-Specialist de als Geprivilegieerd geclaimde gegevens vluchtig inziet, dan zal niet hij, maar de Functionaris Verschoningsrecht, mede aan de hand van de onderbouwing zoals bedoeld in artikel 2, vijfde lid, onder b, van de Werkwijze, beoordelen of de claim aannemelijk is. De leden 1 tot en met 5 van dit artikel zijn in dat geval slechts van toepassing op Privégegevens.

Artikel 4 – Beoordelen van de claim door de Functionaris Verschoningsrecht

1. Het Onderzoekssubject kan het geprivilegieerde karakter van de claim of het gedeelte waarvan de IT-Specialist heeft geoordeeld dat deze niet aannemelijk is, laten beoordelen door de Functionaris Verschoningsrecht. Het Onderzoekssubject dient hiertoe binnen 10 werkdagen na de dagtekening van de kennisgeving zoals bedoeld onder artikel 3, vijfde lid, van de Werkwijze, een gemotiveerd

³ Mocht het Onderzoekssubject het verzoek tot Schonen van Geprivilegieerde gegevens op bestandsniveau wensen te doen, dan dient over de wijze waarop dat verzoek gedaan dient te worden, afstemming met de IT-Specialist plaats te vinden. Zulks binnen de daarvoor in het vierde lid gestelde termijn en voorzien van de onder lid b genoemde onderbouwing.

⁴ Mocht het Onderzoekssubject het verzoek tot Schonen van Privégegevens op bestandsniveau wensen te doen, dan dient over de wijze waarop dat verzoek gedaan dient te worden, afstemming met de IT-Specialist plaats te vinden. Zulks binnen de daarvoor in het vierde lid gestelde termijn en voorzien van de onder lid b genoemde onderbouwing.

verzoek te richten aan de Functionaris Verschoningsrecht.

2. De Functionaris Verschoningsrecht kan het Onderzoekssubject verzoeken een aanvullende toelichting te geven indien er onvoldoende aanknopingspunten zijn om het geprivilegieerde karakter van de betreffende gegevens te beoordelen.
3. Voor zover de Functionaris Verschoningsrecht van oordeel is dat (een gedeelte van) de claim aannemelijk is stelt hij het Onderzoekssubject daarvan schriftelijk in kennis en laat hij de desbetreffende digitale gegevens alsnog Schonen door de IT-Specialist.
4. Indien de Functionaris Verschoningsrecht van oordeel is dat (een gedeelte van) de claim niet aannemelijk is, dan stelt hij het Onderzoekssubject daarvan schriftelijk en gemotiveerd in kennis. In deze kennisgeving geeft de Functionaris Verschoningsrecht aan dat hij de desbetreffende digitale gegevens niet eerder dan 10 werkdagen na verzending van de kennisgeving beschikbaar maakt voor de Onderzoeker. De wachttermijn van 10 werkdagen dient ertoe het Onderzoekssubject de mogelijkheid te bieden een kort geding aanhangig te maken bij de civiele rechter.
5. De correspondentie die tussen het Onderzoekssubject en de Functionaris Verschoningsrecht is gevoerd in het kader van de inhoudelijke beoordeling van de claim is enkel toegankelijk voor de Functionaris Verschoningsrecht.

Artikel 5 – Toezichtonderzoek

1. Het toezichtonderzoek vindt plaats in Geschoonde gegevens.
2. De Onderzoeker voert uitsluitend gerichte zoekacties uit in Geschoonde gegevens.
 - a. Daarbij hanteert de Onderzoeker een zoekstrategie die gebaseerd is op zoektermen.
 - i. De zoektermen vinden hun oorsprong in het doel van het toezichtonderzoek.
 - ii. Bij het verrichten van de zoekacties op basis van de zoektermen, kan gebruik worden gemaakt van technische middelen⁵ om het zoeken efficiënter te laten verlopen.
 - iii. Het Onderzoekssubject kan aan de Onderzoeker verzoeken om een toelichting op de gehanteerde zoekstrategie. Deze toelichting wordt verstrekt nadat de Onderzoeker de gerichte zoekacties heeft afgerond.
 - b. Indien Geschoonde gegevens, gezien het doel van het toezichtonderzoek, in hun totaliteit relevant kunnen zijn⁶, dan zijn de bepalingen onder lid a niet van toepassing.
3. Indien tijdens de gerichte zoekacties in Geschoonde gegevens (onverhoopt) Geprivilegieerde en/of Privégegevens worden aangetroffen, dan zullen deze (alsnog) worden geschoond.
4. De Digitale gegevens die gezien het doel van het toezichtonderzoek als relevant zijn aangemerkt, worden door de IT-Specialist overgedragen aan de Onderzoeker en opgeslagen in het onderzoeks-dossier.

Artikel 6 – Vernietiging van Digitale gegevens

1. De IT-Specialist vernietigt alle van het Onderzoekssubject gekopieerde Digitale gegevens met uitzondering van die digitale gegevens die in het onderzoeksdossier zijn opgenomen:
 - a. zo spoedig mogelijk nadat het toezichtonderzoek is gesloten; of
 - b. zo spoedig mogelijk nadat naar aanleiding van het toezichtonderzoek genomen besluiten, onherroepelijk zijn geworden.
2. Indien Onderzoekssubject zich overeenkomstig artikel 3, zesde lid of artikel 4, eerste lid, van de Werkwijze, gewend heeft tot de Functionaris Verschoningsrecht en de daartoe strekkende claim (al dan niet gedeeltelijk) gehonoreerd is, dan geeft deze opdracht aan de IT-Specialist om de betreffende Geprivilegieerde gegevens te vernietigen en vernietigt deze zelf de daarover gevoerde correspondentie na het geval van en overeenkomstig het eerste lid, onder a of b.

Artikel 7 – Intrekking eerdere Werkwijze

De 'Werkwijze AFM inzien en kopiëren van digitale gegevens', gepubliceerd in de Staatscourant van 9 maart 2020, wordt ingetrokken.

⁵ Hierbij kan worden gedacht aan 'predictive coding' en andere vormen van 'technology assisted review'.

⁶ Hierbij kan worden gedacht aan toezichtonderzoek op basis van controledossiers (Wta) en cliëntdossiers (Wwft).



Artikel 8 – Inwerkingtreding

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

Amsterdam, 2 december 2025

*Autoriteit Financiële Markten,
L.B.J. van Geest
Bestuursvoorzitter*

*H.L. van Beusekom
Bestuurslid*