

FINNIUS

De herziening van de Digitale Werkwijze: stap vooruit of gemiste kans voor rechtsbescherming?

30 april 2026

🕒 11 MINUTEN

Inleiding

Toezicht houden in 2026 betekent in belangrijke mate data verzamelen en analyseren. E-mails, chatgesprekken, bestanden: bij een onderzoek naar mogelijke wetsovertredingen vragen de Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB) doorgaans grote hoeveelheden digitale gegevens op.

Om dit proces te structureren hanteren de toezichthouders een eigen werkwijze voor het veiligstellen en onderzoeken van digitale gegevens: de Digitale Werkwijze.^[1] Deze werkwijze beschrijft hoe digitale onderzoeken ter plaatse worden uitgevoerd en bevat waarborgen voor zowel natuurlijke personen als onder toezicht staande instellingen (het onderzoekssubject). De AFM en DNB hebben de Digitale Werkwijze recent herzien.

Voor instellingen is het van belang te begrijpen wat deze herziening in de praktijk betekent. In deze blog worden de belangrijkste stappen van de Digitale Werkwijze uiteengezet, wordt ingegaan op de belangrijkste wijzigingen ten opzichte van eerdere versies en wordt kritisch bezien in hoeverre de geboden waarborgen daadwerkelijk effectieve rechtsbescherming bieden.

Hoe werkt de Digitale Werkwijze in de praktijk?

De Digitale Werkwijze beschrijft stap voor stap hoe de AFM en DNB te werk gaan wanneer zij digitale gegevens opvragen en onderzoeken.

Als eerste stelt de onderzoeker, een toezichthouder van de AFM of DNB, vast welke digitale gegevens nodig zijn voor het onderzoek. De IT-specialist – eveneens een toezichthouder van de AFM of DNB, maar die niet betrokken is bij het inhoudelijke onderzoek – kopieert de relevante gegevens, transporteert deze versleuteld naar de AFM of DNB en slaat ze op in een afgeschermd omgeving. De onderzoeker heeft op dat moment nog geen toegang tot deze gegevens.^[2]

Binnen vijf werkdagen na het kopiëren ontvangt het onderzoekssubject een overzicht van de gekopieerde gegevens. Daarbij wordt gewezen op de mogelijkheid een schoningsverzoek in te dienen.^[3] Het onderzoekssubject heeft tien werkdagen om schriftelijk te verzoeken dat geprivilegieerde gegevens (correspondentie met een advocaat, arts, notaris of geestelijke) en/of privégegevens worden uitgesloten van het onderzoek.^[4] Als geen verzoek wordt ingediend, voert de IT-specialist indien nodig een pro-forma-schoning uit om geprivilegieerde gegevens te verwijderen.^[5]

De IT-specialist beoordeelt vervolgens het schoningsverzoek: eerst op basis van metadata^[6] en alleen 'waar nodig' door middel van vluchtig inzien. Als de schoning plaatsvindt op kantoor van de toezichthouder (wat doorgaans zo zal zijn), krijgt het onderzoekssubject een mondelinge toelichting over de wijze waarop de schoning is voorbereid en wordt uitgevoerd.^[7]

Indien het onderzoekssubject bezwaar heeft tegen vluchtig inzien door de IT-specialist, of het niet eens is met diens oordeel, kan het de zaak voorleggen aan de functionaris verschoningsrecht.^[8] Deze functionaris verschoningsrecht is niet betrokken bij het toezichtonderzoek (maar wel werkzaam bij de AFM/DNB). Acht ook deze functionaris de claim niet aannemelijk, dan stelt hij het onderzoekssubject daarvan gemotiveerd in kennis en kondigt hij aan dat de gegevens na tien werkdagen beschikbaar worden gesteld aan de toezichthouder die het onderzoek verricht. Die termijn biedt het onderzoekssubject de gelegenheid een kort geding bij de civiele rechter aanhangig te maken.^[9]

Het eigenlijke onderzoek vindt uitsluitend plaats op basis van de geschoonde gegevens. De onderzoeker werkt op basis van gerichte zoektermen die, als het goed is, direct verband houden met het doel van het onderzoek. Het onderzoekssubject kan alleen achteraf een toelichting vragen op de gehanteerde zoekstrategie. Gegevens die relevant zijn voor het onderzoek worden overgedragen aan de onderzoeker en opgeslagen in het onderzoeksdossier.^[10]

Na afronding van het onderzoek worden alle gekopieerde gegevens die niet in het onderzoeksdossier zijn opgenomen zo spoedig mogelijk vernietigd – maar pas nadat het onderzoek is gesloten of eventuele besluiten onherroepelijk zijn geworden.^[11]

Wat is er nieuw ten opzichte van de werkwijze uit 2020?

De vorige versies van de Digitale Werkwijze dateerden uit 2020 en sloten volgens de toezichthouders niet meer aan op de huidige toezichtpraktijk. In de vernieuwde versies zijn rollen en processen helderder beschreven, is de positie van de IT-specialist en de functionaris verschoningsrecht verduidelijkt, en is expliciet vastgelegd hoe wordt omgegaan met privé- en geprivilegieerde gegevens – aldus de toezichthouders.^[12]

De meest in het oog springende wijziging is de introductie van de pro-forma-schoning. Onder de oude werkwijze kreeg de onderzoeker in principe toegang tot alle gekopieerde gegevens als het onderzoekssubject geen schoningsverzoek indiende. Dat is nu anders: volgens de website van de AFM voert de IT-specialist voortaan standaard een pro-forma-schoning van geprivilegieerde gegevens uit, ook zonder dat daarom is verzocht.

Ook de beoordeling door de IT-specialist is genuanceerder geworden. Waar hij in 2020 standaard begon met vluchtig inzien van de geclaimde gegevens, kijkt hij nu eerst naar metadata. Alleen 'waar nodig', mag hij de gegevens vluchtig inzien. Dit beperkt de inbreuk op het verschoningsrecht volgens de AFM tot wat strikt noodzakelijk is.

Verder is de informatieverplichting richting het onderzoekssubject aangescherpt. Als de schoning ten kantore van de AFM of DNB plaatsvindt, krijgt het onderzoekssubject nu een actieve mondelinge toelichting over de voorbereiding en uitvoering van de schoning, waar voorheen slechts de mogelijkheid bestond om aanwezig te zijn.

Tot slot zijn de rollen van de IT-specialist en de functionaris verschoningsrecht scherper omschreven, en is de onafhankelijkheid van beide functionarissen ten opzichte van het toezichtonderzoek expliciet verankerd. Het toezichtonderzoek zelf vindt uitdrukkelijk uitsluitend plaats in de geschoonde gegevens, iets wat in de oude werkwijze minder expliciet was vastgelegd.

Hoe zit het met de rechtsbescherming?

De AFM en DNB presenteren de vernieuwde Digitale Werkwijze als een verbetering voor het onderzoekssubject. En dat is zij op onderdelen ook. De pro-forma-schoning en de metadata-first benadering zijn stappen in de goede richting. Tegelijkertijd kunnen ook bij de aangepaste werkwijzen de nodige kanttekeningen worden geplaatst.

Zo schrijft de AFM op haar website dat de pro-forma-schoning voortaan standaard plaatsvindt, maar de werkwijze zelf is genuanceerder: de IT-specialist voert de pro-forma-schoning uit “indien nodig.” Evenzo mag de IT-specialist de geclaimde gegevens “waar nodig” vluchtig inzien. Het is dus nog de vraag hoe deze open normen in de praktijk worden ingevuld: wanneer is een pro-forma-schoning nodig, en wanneer is vluchtig inzien noodzakelijk? De praktijk zal moeten uitwijzen of de beoogde terughoudendheid ook daadwerkelijk wordt betracht.

Maar ook los daarvan rijst de vraag of de geboden waarborgen überhaupt voldoen aan de normen die de Hoge Raad, het EHRM en het Hof van Justitie stellen. De volgende punten verdienen nadere aandacht:

De functionaris verschoningsrecht: onafhankelijk genoeg?

Een eerste punt van aandacht is de rol van de functionaris verschoningsrecht. De werkwijzen van de AFM en DNB beschrijven hem als een onafhankelijke functionaris die buiten het onderzoeksteam staat. Maar de functionaris verschoningsrecht blijft een medewerker van dezelfde instelling die het onderzoek voert. Het EHRM oordeelde al in 2010 dat toetsing van het geprivilegieerde karakter van gegevens moet plaatsvinden door een “*judge or other independent and impartial decision-making body*.”^[13] Het is zeer de vraag of een interne functionaris, hoe zorgvuldig ook gepositioneerd, aan die maatstaf voldoet.

De Hoge Raad: een centrale rol voor de rechter

Die twijfel wordt versterkt door de prejudiciële beslissing van de Hoge Raad van 12 maart 2024, gewezen in de strafzaak Castor.^[14] De Hoge Raad formuleerde daarin duidelijke uitgangspunten: ambtenaren van een opsporings- of toezichtsinstantie mogen in beginsel geen kennis nemen van mogelijk geprivilegieerde gegevens, en de selectie en beoordeling daarvan is in beginsel voorbehouden aan de rechter-commissaris. Hoewel die beslissing betrekking had op het strafrecht (en het bestuursrecht ook geen rechter-commissaris kent), zijn de onderliggende rechtsvragen rechtsgebiedoverstijgend. Het verschoningsrecht is een algemeen rechtsbeginsel^[15] dat in alle

rechtsgebieden geldt, en de uitgangspunten van de Hoge Raad zijn daarmee ook relevant voor bestuursrechtelijke toezichthouders als de AFM en DNB.^[16] De Autoriteit Consument en Markt (ACM) heeft bijvoorbeeld naar aanleiding van de Castor-zaak ook haar werkwijze voor de omgang met (mogelijk) geprivilegieerde gegevens aangepast.^[17] Zo is het onder deze nieuwe werkwijze niet meer mogelijk om met een ‘vluchtige blik’ kennis te nemen van geprivilegieerd materiaal, wat voorheen wel het geval was. Op dit punt gaat de ACM dus verder dan de financiële toezichthouders.

Waarborgen op papier

De Castor-zaak illustreert bovendien een ander risico: het verschil tussen formele waarborgen en de praktische werkelijkheid. In die zaak bleek dat een “met waarborgen omklede bestendige werkwijze” in de praktijk niet bestond of niet werkte. Opsporingsambtenaren namen structureel kennis van geprivilegieerde gegevens, in strijd met de eigen interne regels. De rechter stelde in deze zaak vast dat de scheiding tussen opsporingsambtenaren en functionarissen verschoningsrecht “met name op papier leek te bestaan zonder voldoende waarborgen voor de praktijk op de werkvloer.” Interne werkwijzen, hoe zorgvuldig ook geformuleerd, bieden daarom geen garantie dat dit in de praktijk ook zo werkt. Of de functionaris verschoningsrecht en de onderzoeker in de praktijk daadwerkelijk gescheiden zijn, blijft voor het onderzoekssubject oncontroleerbaar.

Het initiatief ligt bij het onderzoekssubject

Hét probleem uit oogpunt van rechtsbescherming is en blijft dat een informatieverzoek geen besluit oplevert in de zin van de Awb, waardoor onderzoekssubjecten in beginsel daartegen niet in bezwaar en beroep kunnen.

De werkwijzen van de AFM en DNB voorzien wel in een wachtermijn van tien werkdagen waarbinnen het onderzoekssubject een kort geding (bij de civiele rechter) kan aanspannen als de functionaris verschoningsrecht een claim afwijst. Maar het initiatief ligt daarmee volledig bij het onderzoekssubject zelf. Uit de jurisprudentie volgt nu juist dat de staat proactief alles moet doen om inbreuk op het verschoningsrecht te voorkomen.^[18]

Een mogelijke uitweg is het indienen van een handhavingsverzoek dat op zichzelf betrekking heeft: door de toezichthouder te verzoeken handhavend op te treden tegen zichzelf, kan een voor bezwaar en beroep vatbaar besluit worden uitgelokt.

Verwijderen van de gegevens ‘zo spoedig mogelijk’

Tot slot geldt op grond van de Digitale Werkwijze dat na afronding van het onderzoek alle gekopieerde gegevens die niet in het onderzoeksdossier zijn opgenomen zo spoedig mogelijk worden vernietigd. Dit is pas nadat het onderzoek is gesloten of eventuele besluiten onherroepelijk

zijn geworden. Dat betekent in de praktijk dat de toezichthouder ook geprivilegieerde gegevens (zoals vertrouwelijke correspondentie met een advocaat) jarenlang kan bewaren, zelfs wanneer een verschoningsrechtclaim is gehonoreerd. Dit wringt: art. 5:20 Awb bepaalt dat toezichthouders geen recht hebben op inzage in geprivilegieerde gegevens – het bewaren ervan tot een besluit onherroepelijk is, staat daarmee op gespannen voet.

Conclusie

De vernieuwde werkwijzen van de AFM en DNB bevatten kleine verbeteringen. Maar zolang de beoordeling van geprivilegieerde gegevens volledig intern blijft en rechterlijke betrokkenheid afhankelijk is van eigen initiatief van het onderzoekssubject, valt te betwijfelen of het verschoningsrecht in de bestuursrechtelijke toezichtpraktijk voldoende is gewaarborgd. Voor instellingen die met een digitaal onderzoek worden geconfronteerd, is het verstandig om vroegtijdig juridisch advies in te winnen en waar nodig actief gebruik te maken van de rechtsmiddelen die de Digitale Werkwijze biedt. Daarnaast kan het indienen van een handhavingsverzoek dat op zichzelf betrekking heeft een uitkomst bieden, om zo een voor bezwaar en beroep vatbaar besluit uit te lokken. Finnius informeert instellingen hier graag over.

[1] Alhoewel beide toezichthouders een eigen werkwijze hebben, zijn ze vrijwel identiek.

[2] De Digitale Werkwijze, artikel 2 lid 1 en 2.

[3] De Digitale Werkwijze, artikel 2 lid 3.

[4] De Digitale Werkwijze, artikel 2 lid 4.

[5] De Digitale Werkwijze, artikel 2 lid 8.

[6] Metadata is informatie die eigenschappen of kenmerken van andere data beschrijft.

[7] De Digitale Werkwijze, artikel 3 lid 1 t/m 3.

[8] De Digitale Werkwijze, artikel 4.

[9] De Digitale Werkwijze, artikel 4 lid 4.

[10] De Digitale Werkwijze, artikel 5.

[11] De Digitale Werkwijze, artikel 6.

[12] Zie de toelichting van de AFM hier <https://www.afm.nl/nl-nl/sector/actueel/2025/dec/sb-digitale-werkwijze> en de toelichting van DNB hier <https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2025/q4/dnb-past-digitale-werkwijze-aan/>.

[13] EHRM 14 september 2010, nr. 38224/03, NJ 2011/230, m.nt. E.J. Dommering en T.M. Schalken (Sanoma/Nederland).

[14] HR 12 maart 2024, ECLI:NL:HR:2024:375 (*Castor*).

[15] Het Hof van Justitie van de Europese Unie heeft in zijn arrest van 26 september 2024 bevestigd dat zowel artikel 7 van het Handvest van de grondrechten van de Europese Unie als artikel 8, eerste lid, van het Europees Hof voor de Rechten van de Mens een bijzondere bescherming toekennen aan het verschoningsrecht van advocaten. Ongeacht het rechtsgebied valt juridisch advies van een advocaat onder de versterkte bescherming van artikel 7 van het Handvest, die strekt tot waarborging van de vertrouwelijkheid van de communicatie tussen advocaat en cliënt.

[16] Zie bijv. concl. A-G Timmermans 3 januari 2020, ECLI:NL:PHR:2020:14, punt 2.19 e.v.

[17] <https://www.acm.nl/nl/publicaties/acm-werkwijze-geheimhoudingsprivilege-advocaat-2024>.

[18] *Castor* uitspraak 6.5.1.

Specialisten



Masha Advan

T +31 (0)20 767 01 80

M +31 (0)6 29 27 49 33

masha.advan@finnius.com