STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 32814
22 juni 2020

# DNB Werkwijze inzien en kopiëren van digitale gegevens

De door De Nederlandsche Bank (DNB) aangewezen toezichthouders zijn belast met het toezicht op de naleving van de bij en krachtens (onder meer) de Wet op het financieel toezicht (Wft) gestelde regels. Daartoe beschikken deze toezichthouders op grond van de Algemene wet bestuursrecht (Awb) over de bevoegdheid om inzage te vorderen van zakelijke gegevens en bescheiden en daarvan kopieën te maken (artikel 5:17 Awb). Ook zijn zij bevoegd om inlichtingen te vorderen (artikel 5:16 Awb). De onderneming waarbij een onderzoek wordt verricht, is verplicht alle medewerking te verlenen die redelijkerwijs bij de uitoefening van deze bevoegdheden kan worden gevorderd (artikel 5:20 Awb). Personen die een beroep kunnen doen op een verschoningsrecht, zoals advocaten, kunnen medewerking weigeren (artikel 5:20, lid 2 Awb). Verder vereist het evenredigheidsbeginsel dat een toezichthouder van zijn bevoegdheden slechts gebruik maakt voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is (artikel 5:13 Awb).

Deze Werkwijze geeft op hoofdlijnen weer hoe de toezichthouders van DNB te werk zullen gaan bij het uitoefenen van genoemde bevoegdheden voor zover DNB daarbij digitale gegevens vordert. De Werkwijze is van overeenkomstige toepassing op het vorderen van digitale gegevens op grond van artikel 5:16 van de 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.

## Artikel 1 – Definities

*Awb:* de Algemene wet bestuursrecht.
*Digitale gegevens:* elektronische gegevens waarover het Onderzoekssubject beschikt of kan beschikken.
*Functionaris Verschoningsrecht:* een door een directielid van De Nederlandsche Bank (DNB) aangewezen persoon die niet als IT-Specialist of als Onderzoeker bij onderzoeken betrokken is of zal zijn en onafhankelijk van het toezicht het geprivilegieerde karakter van de door het Onderzoekssubject geclaimde gegevens toetst.
*Geprivilegieerde gegevens:* Digitale gegevens die zijn gewisseld tussen een Onderzoekssubject en diens advocaat in die hoedanigheid. De gegevens worden als geprivilegieerd aangemerkt wanneer de advocaat zich ten aanzien van die gegevens zou kunnen beroepen op het verschoningsrecht[1] 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 tevens belast is met het proces van identificeren, veiligstellen, kopiëren en verwerken van Digitale gegevens en die niet betrokken is bij de inhoudelijke uitvoering van het toezichtonderzoek.
*Onderzoeker:* een toezichthouder in de zin van artikel 5:11 Awb die het toezichtonderzoek uitvoert.
*Onderzoekssubject:* de natuurlijke persoon of rechtspersoon van wie in het kader van een informatievordering Digitale gegevens worden veiliggesteld en gekopieerd.
*Privégegevens:* Digitale gegevens en bescheiden die persoonsgegevens en/of persoonlijke informatie bevatten en niet als zakelijke gegevens kwalificeren zoals bedoeld in artikel 5:17 Awb.
*Schonen / Schoning:* het uitsluiten van Geprivilegieerde- en/of Privégegevens uit de verzameling van veiliggestelde en gekopieerde digitale gegevens.
*Werkwijze:* de Werkwijze DNB inzien en kopiëren van digitale gegevens.

## Artikel 2 – Identificeren, veiligstellen en kopiëren van Digitale gegevens ter plaatse

1. De Onderzoeker stelt, aan de hand van het doel van het onderzoek, vast welke Digitale gegevens worden gevorderd van het Onderzoekssubject. De IT-Specialist draagt er zorg voor dat deze Digitale gegevens worden geïdentificeerd, veiliggesteld en gekopieerd.

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

2. De van het Onderzoekssubject gekopieerde Digitale gegevens worden door de IT-Specialist op versleutelde wijze getransporteerd en 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 zij[2] DNB schriftelijk verzoeken om deze gegevens te Schonen. Dit verzoek dient uiterlijk 10 werkdagen na verzending van de in het derde lid genoemde kennisgeving gericht te worden aan de IT-Specialist of, indien toepassing wordt gegeven aan artikel 3, zesde lid, van de Werkwijze, aan de Functionaris Verschoningsrecht.

5. Het in het vierde lid genoemde verzoek dient de volgende informatie te bevatten:
   a) gegevens over de auteur en het onderwerp. In geval van correspondentie tevens gegevens over de afzender, de geadresseerde en het moment van verzending (datum & tijd), en
   b) een deugdelijke onderbouwing waaruit blijkt dat er sprake is van verschoningsgerechtigde 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 de volgende informatie te bevatten:
   a) gegevens over de auteur en het onderwerp. In geval van correspondentie tevens gegevens over de afzender, de geadresseerde en het moment van verzending (datum & tijd), 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 geeft de Onderzoeker daarna toegang tot de Digitale gegevens.

**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 middel van vluchtig inzien beoordelen of de claim terecht voorkomt.

2. De Schoning vindt in beginsel plaats op de plek waar de gekopieerde Digitale gegevens door DNB zijn opgeslagen. 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. De IT-Specialist het Onderzoekssubject in de gelegenheid om tijdens de Schoning aanwezig te zijn.

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 gegrond is, stelt de IT-Specialist het Onderzoekssubject daarvan schriftelijk in kennis en schoont de IT-Specialist de terecht geclaimde digitale gegevens.

6. Indien het Onderzoekssubject stelt dat het vluchtig inzien van de als verschoningsgerechtigd geclaimde gegevens door de IT-Specialist het verschoningsgerechtigde karakter kan schaden, dan

[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.

zal 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 terecht voorkomt. 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 onterecht 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 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 terecht 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 onterecht 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 – Onderzoek van de Geschoonde gegevens**

1. Na afronding van de Schoning, en indien van toepassing, het verstrijken van de in artikel 4 lid 4 bedoelde termijn, geeft de IT-Specialist de Onderzoeker toegang tot de Geschoonde gegevens.

2. De Onderzoeker voert uitsluitend gerichte zoekacties uit in de 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 onderzoek.
      ii. Bij het verrichten van de zoekacties op basis van de zoektermen, kan gebruik worden gemaakt van technische middelen[3] om het zoeken efficiënter te laten verlopen.
      iii. Op verzoek van het Onderzoekssubject wordt een toelichting verschaft op de gehanteerde zoekstrategie.
   b) Indien de Geschoonde gegevens, gezien het doel van het onderzoek, in hun totaliteit relevant kunnen zijn[4], dan zijn de bepalingen onder lid a niet van toepassing.

3. Indien tijdens het onderzoek in de Geschoonde gegevens (onverhoopt) Geprivilegieerde- en/of Privégegevens worden aangetroffen, dan zullen deze (alsnog) worden geschoond.

4. De Geschoonde gegevens die gezien het doel van het onderzoek als relevant zijn aangemerkt, worden door de IT-Specialist overgedragen aan de Onderzoeker en opgeslagen in het onderzoeksdossier.

**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 onderzoek genomen besluiten, onherroepelijk zijn geworden.

2. Indien het Onderzoekssubject zich overeenkomstig artikel 3, zesde lid of artikel 4, eerste lid, van de

[3] Hierbij kan worden gedacht aan 'predictive coding' en andere vormen van 'technology assisted review'.
[4] Hierbij kan worden gedacht aan onderzoek op basis van cliëntdossiers (Wwft).

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 – Inwerkingtreding**

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

*Amsterdam, 2 juni 2020*

*De Nederlandsche Bank N.V.*
*F. Elderson*
*Directeur Toezicht*